Summary of the FFM Workshop at EUROCONTROL

An invitation-only workshop on Cyber Frameworks, Mappings and Metrics was hosted by EUROCONTROL on 23 January, 2020. It was organized by EUROCONTROL, Freddy Dezeure and Josh Magri of BPI/Cyber Risk Institute.

It was the first of its kind, offering CISOs (Chief Information Security Officer) and Regulators/Competent Authorities of four critical sectors (finance, telecom, transport and energy) an opportunity to exchange practical experiences in implementing frameworks customized with applicable regulatory and control mappings and metrics.

The workshop was well attended, with 140 participants and 18 speakers from Europe and the United States. Apart from private sector user organizations, there were also attendees from the European Commission, ENISA, regulatory agencies, national CERTs (Computer Emergency Response Team) and sectoral ISACs (Information Sharing and Analysis Center).

Cyber security frameworks are considered a useful tool to approach cybersecurity challenges in a coherent and exhaustive manner and to design and implement a corporate cyber security strategy.

In many jurisdictions, cybersecurity regulations have been issued with compliance obligations for “critical” infrastructure. Many multi-national organisations must comply with several of these requirements, because of their geographical spread. Many organisations are also required to comply with sectoral regulatory requirements and these can vary significantly by country or region. A good example is the financial sector, with myriad regulations imposing differently worded, but similarly intentioned requirements across the globe.

All the speakers echoed the burden that this poses on their organisation. A 2016 survey facilitated by the FSSCC (Financial Services Sector Coordinating Council and FS-ISAC (Financial Sector ISAC) revealed that CISOs and their teams spend at least 40% of their time on compliance activities addressing similar concerns but needing to tailor responses to slightly different requests.

To address this challenge given the well documented shortage of cyber expertise, the financial services sector developed Financial Sector Profile as a potential solution (with potential multi-sector application), using mappings between different Frameworks as well as mappings toward regulatory requirements worldwide. This model and its practical implementation were illustrated by several speakers and enthusiastically received by the audience. The overwhelming response from the audience was that a similar approach could and should be followed in the other sectors.

In addition, the speakers and the audience indicated that differences in cybersecurity challenges/controls between sectors are not as important as people may (initially) believe. Lack of understanding or knowledge of existing models and mappings still leads to duplication of efforts and the design of new Frameworks and standards. Ultimately, whichever sector, regulatory requirements, frameworks and standards, the vast majority of security controls-are common because so is the information and operations technology (IT/OT).

The workshop also attempted to include the Regulators. Agency representatives joined in the debate, generally agreeing on a more harmonized approach but cautioning

 not to trade security for alignment or “blind spots”. Nonetheless, it was clear that the development of Acceptable Means of Compliance to sector regulatory requirements and

standards should rely much more on such existing frameworks instead of reinventing the wheel. The effort should be more focussed on their implementation.

The third subject of the workshop was Metrics, used in conjunction with Frameworks, to give control to the CISO, report to his C-suite or demonstrate compliance. Some of the speakers from the financial sector hinted at the existence in their organisation of KPIs (Key Performance Indicator) and KRIs (Key Risk Indicator) for the subcategories of the Framework they use. A few speakers gave examples of the Metrics they use.

The Metrics discussion was a bit limited, but all agreed that metrics is a key topic and area for future cooperation and development. Most attendees and speakers agreed on the need to have Metrics to "objectivize" and automate the completion of Framework content, replacing to a certain extent self-assessment and diagnostic statements. But most also agree that they don't have this in place for the moment.

Using inappropriate metrics would lead organizations to spend resources, effort and time addressing the wrong problems at the outset and potentially future business cycles, as senior management look for consistency in the metrics used and improvement over time. Proposed actions

1. Raise awareness on existing good practices in Frameworks and Mappings
    a. By ISACs towards their members
    b. By national and sectorial CERTs towards the CSIRT network and competent authorities
    c. Towards the EU legislator
    d. Produce and release a White Paper
2. Extend the Financial Profile with the European scope and use the model to achieve the same goal for other sectors
    a. By ISACs
    b. By standardisation bodies
    c. By the Cyber Risk Institute per request
3. Involve regulators/Competent Authorities in the debate, cross-sector and crossnation
    a. Promote those frameworks and metrics to the regulatory community at global, regional, national sectorial organisation as well as National Cybersecurity Authorities
    b. Educate regulators/Competent Authorities to those improved approaches
    c. Ensure that regulators consider those frameworks and metrics as AMC and Guidance Material to new or existing regulatory requirements
4. Organise a similar workshop focussed on Metrics