WORLD BANK GROUP
Finance & Markets
Financial Sector Advisory Center (FinSAC)

Cyber-Security Survey

SELF-ASSESSMENTS

AQUILES A. ALMANSI

THE WORLD BANK

Objective and Scope

The objective of the World Bank Group's Vienna Center for Financial Sector Advisory Services (FinSAC) survey was to contribute to cyber-risk awareness and preparedness.

Fifteen Central Banks were invited to comment on cyber incidents in their respective jurisdictions, and to assess the current state of their own cyber security practices. The results reported here correspond to the fourteen responses received.

FinSAC took as a model OSFI's cyber security self-assessment questionnaire.

Main Findings – Information on Incidents

- Eleven of the fourteen respondents have been target of cyber-attacks. Of these, all but one have registered incidents of actual network penetration, and at least three are regularly blocking (from daily to once or twice a week) attacks.
- Knowledge about cyber-attack attempts and successful breach incidents of financial institutions in their respective jurisdictions varies considerably across the fourteen countries. No information In five of them.
- Ten of fourteen respondents reported to have no information about cyber-attacks to major utility providers, retail stores, or other public or private institutions holding customer bank or credit card data.

Main Findings – Self Assessments

- The strongest self-assessments correspond to technical issues typically in charge of IT departments.
- The weakest self-assessments correspond to areas typically in the hands of Senior Management and/or the Governor/Board, with institutional developmental issues similar to those frequently present in every other area of financial regulation and supervision.
- Self-assessments were far from unanimous, the highest dispersion corresponding to areas with the weakest self-assessments.

Self-Assessment Ratings:

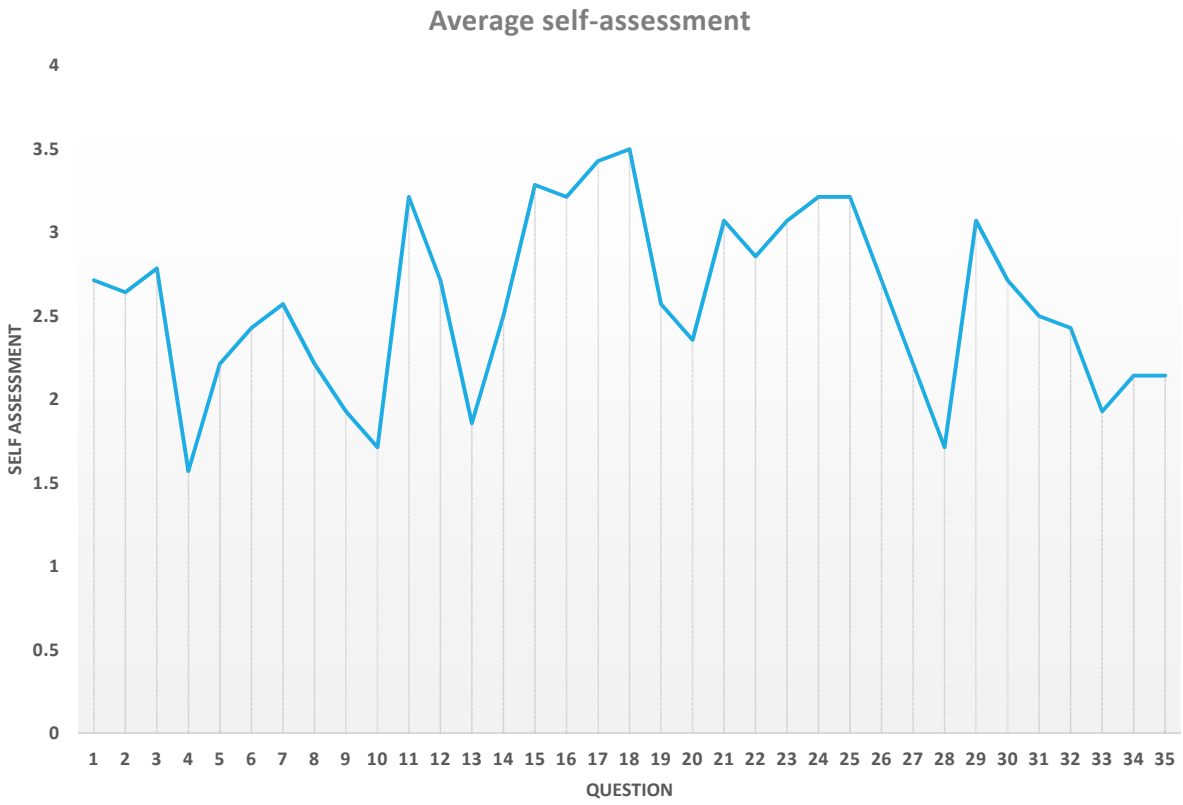
4. Fully Implemented

3. Largely Implemented

2. Partially Implemented

1. Not Implemented

0. NA



Strongest Self-Assessments

Q18, avg. 3.50: The Central Bank segments its network into multiple, separate trust zones.

Q17, avg. 3.43: The Central Bank has implemented network boundary monitoring and protection.

Q15, avg. 3.29: The Central Bank has implemented the following security tools and provides for their automated updates, and institution-wide application: Intrusion detection / protection systems; Web application firewalls; Anti-virus; Anti-spyware; Anti-spam; DDoS protection; other.

Q25, avg. 3.21: The Central Bank tightly controls the use of administrative privileges.

Q24, avg. 3.21: The Central Bank applies strong authentication mechanisms to manage user identities and access.

Q16, avg. 3.21: The Central Bank has a process to obtain, test and automatically deploy security patches and updates in a timely manner.

Q11, avg. 3.21: The Central Bank maintains current a knowledge base of its users, devices, applications and their relationships, including but not limited to software and hardware assets, network maps (including boundaries, traffic and data flow), and network utilization and performance data.

Q29, avg. 3.07: The Central Bank's incident management process is designed to ensure that the following tasks are fully completed: Recovery from disruption of services; Assurance of systems' integrity following the cyber security incident; Recovery of lost or corrupted data.

Weakest Self-Assessments

Q4, avg. 1.57: Cyber security awareness is provided to all commercial bank employees.

Q10, avg. 1.71: The Central Bank conducts regular cyber-attack and recovery simulation exercises.

Q28, avg. 1.71: The Central Bank has an external communication plan to address cyber security incidents that includes communication protocols and draft pre-scripted communications for key external stakeholders (i.e. customers, media, critical service providers, etc.

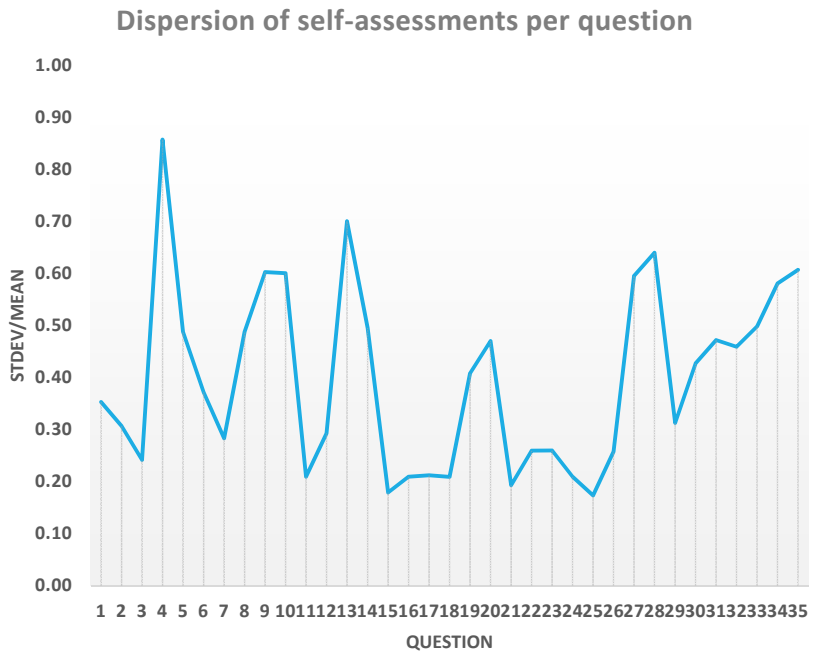
Q13, avg. 1.86: 'The Central Bank monitors and tracks cyber security incidents in the financial services industry and other relevant sectors.

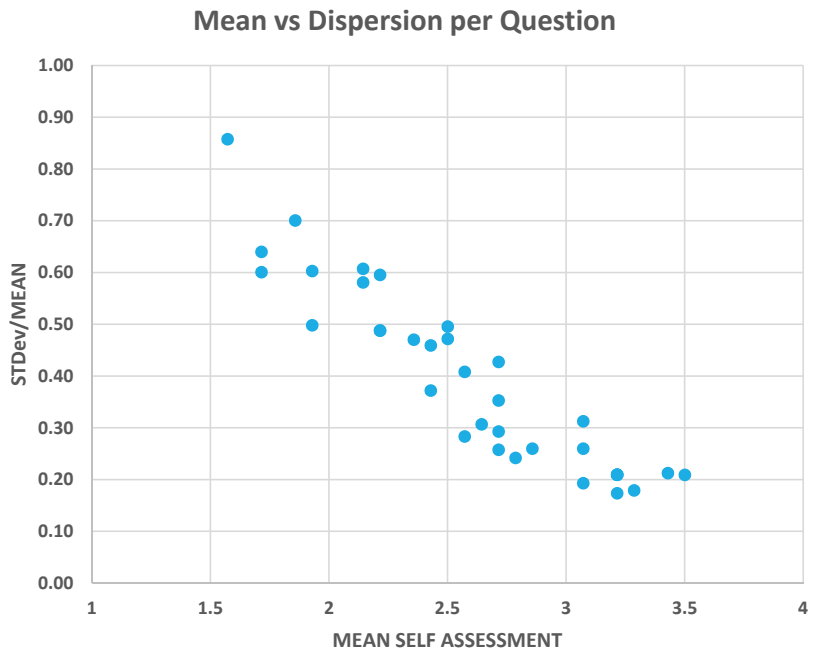
Q9, avg. 1.93: The Central Bank conducts regular testing with third party cyber-risk mitigating services.

Q33, avg. 1.93: The Central Bank has utilized scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.

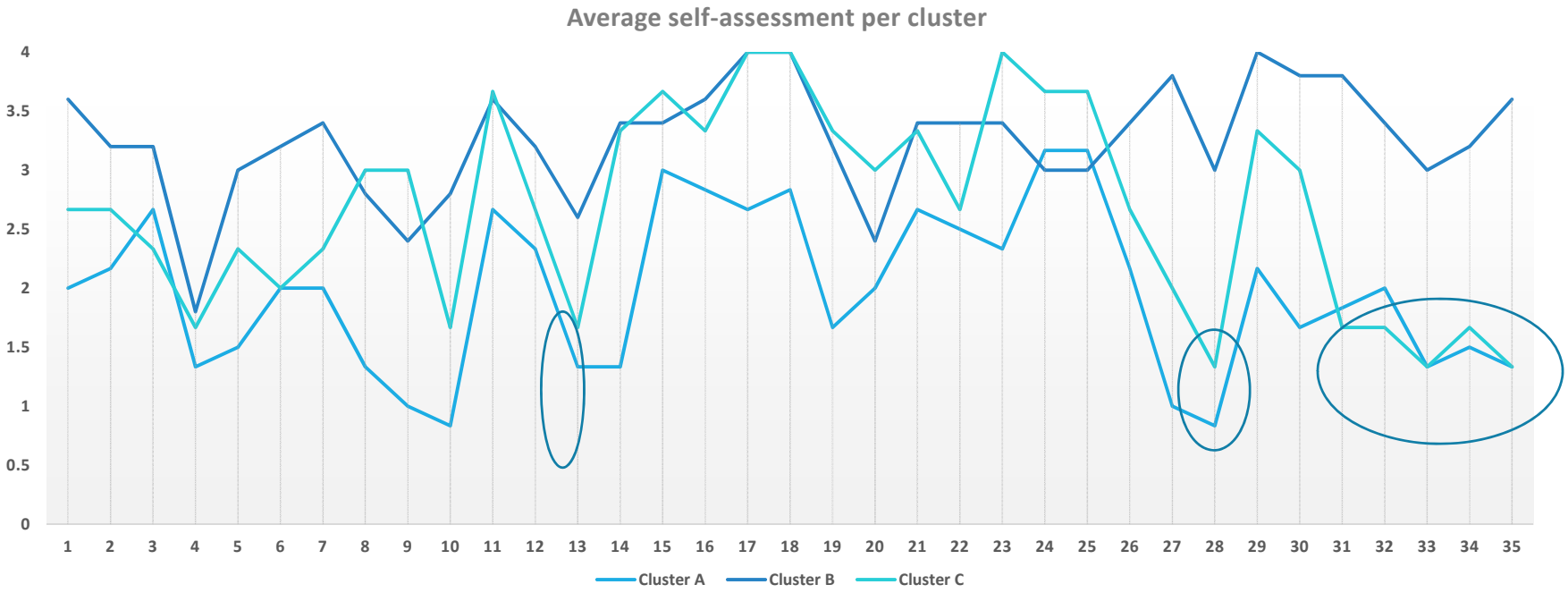
Q34, avg. 2.14: A Senior Management committee has been established that is dedicated to the issue of cyber risks, or an alternative Senior Management committee has adequate time devoted to the discussion of the implementation of the cyber security framework.

Dispersion of Self-Assessments





Understanding the dispersion



Areas of greatest dispersion

13. The Central Bank monitors and tracks cyber security incidents in the financial services industry and other relevant sectors.

28. The Central Bank has an external communication plan to address cyber security incidents that includes communication protocols and draft pre-scripted communications for key external stakeholders (i.e. customers, media, critical service providers, etc.).

31. The Central Bank has established an institution-wide cyber security policy, with supporting procedures in place that set forth how the Central Bank will identify and manage its cyber security risks.

32. The Central Bank has a cyber-security implementation plan that outlines key initiatives and timelines.

33. The Central Bank has utilized scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.

34. A Senior Management committee has been established that is dedicated to the issue of cyber risks, or an alternative Senior Management committee has adequate time devoted to the discussion of the implementation of the cyber security framework.

35. The Board, or a committee of the Board, is engaged on a regular basis to review and discuss the implementation of the Central Bank's cyber security framework and implementation plan, including the adequacy of existing mitigating controls.

Conclusions

Information on cyber security-events: good about incidents affecting the Central Bank, limited about incidents affecting supervised institutions, very limited or inexistent about incidents affecting other sectors.

Self-Assessments: the strongest correspond to issues typically in charge of IT departments, the weakest self-assessments correspond to areas typically in the hands of Senior Management and/or the Governor/Board.