WORLD BANK GROUP
Finance & Markets

Financial Sector Advisory Center (FinSAC)

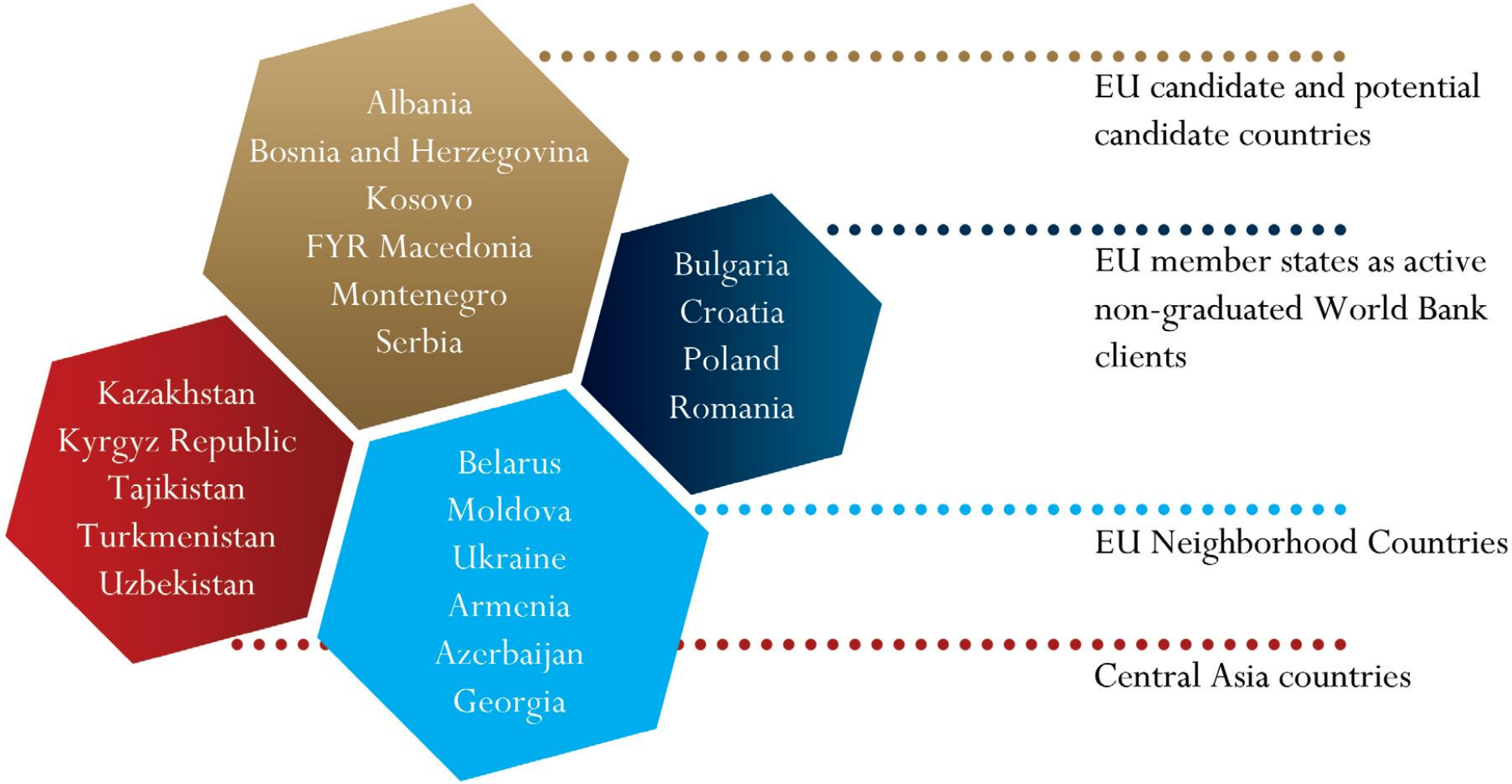
Cyber-Crisis Preparedness and Management in the Financial Sector

Aquiles A. Almansi
Lead Financial Sector Specialist

What is FinSAC?

- The Vienna Financial Sector Advisory Center (FinSAC) is a technical unit of the World Bank's Finance & Markets Global Practice funded by the Austrian Government.
- FinSAC provides policy and technical advice, as well as analytical services, to client countries in Emerging Europe and Central Asia.
- Growing concern on cyber-security touches two of FinSAC's main work areas: 1) financial stability/crisis prevention, and 2) financial regulation/supervision.

FinSAC Client Countries



Cyber Crime in the Financial Sector

Cyber is the fastest growing among the five most frequent economic crimes affecting the financial sector:

	2016	2014
Asset misappropriation	60%	67%
Cybercrime	**49%**	**39%**
Money Laundering	24%	24%
Accounting Fraud	18%	21%

Source: PwC's Global Economic Crime Survey 2016

http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/financial-services-insights.html

1.Prof. Malcoln Sparrow

What do we see on cyber preparedness and crisis management?

- FinSAC's 2015 survey on cyber preparedness among Central Banks of 15 client countries.
- Attitudes towards cyber-incidents observed in financial-crisis simulation exercises around the world, including 10 with FinSAC client countries.
- Accenture's survey among the 109 largest banks in the world.
- Increasingly detailed Initiatives by regulators and private sector groups.

FinSAC's 2015 Survey: interesting facts

- Eleven of the fourteen respondents acknowledged to have been targets of cyber-attacks.
- Knowledge about cyber-attack attempts and successful breach incidents of financial institutions in their respective jurisdictions varied 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.

FinSAC's 2015 Survey: self assessments

- **Strongest self-assessments in technical matters in charge of IT departments:** networks segmented into multiple trust zones, security software automatically updated, etc.
- **Weakest self-assessments in the matters in the hands of Senior Management and/or the Governor/Board**: no cyber security awareness training required from supervised institutions, no regular cyber-attack and recovery simulation exercises, no external communication plan to address cyber security incidents, no regular testing with third party cyber-risk mitigating services, etc.

WB-FinSAC Crisis Simulation Exercises

- The WB has run more than 30 financial crisis simulation exercises around the world since 2008, including 10 with FinSAC client countries. These are “war games” for Ministers of Finance, Central Bank Governors, Heads of Bank Supervision, and other senior officials from national financial sector authorities to practice communication and coordination in their decision making process.
- Our more recent crisis scenarios frequently involve cyber incidents as triggers for conventional banking problems. Typical responses are consistent with the self assessments: authorities are (more or less) ready to cope with the liquidity/solvency consequences of a cyber incident, but they tend to see no role for themselves in managing the incident.

Accenture's report

"...less than 6% of boardroom members and 3% of CEOs at the world's 109 largest banks have professional technology experience..."

https://thefinancialbrand.com/60578/technology-expertise-banking-boardrooms

Public and Private Initiatives

- **Public**: for example the joint "Advance Notice of Proposed Rulemaking" issued by the Federal Reserve Board, the OCC and the FDIC last month on cyber risk management standards, emphasizing the importance of cyber-risk governance, and similar initiatives by other regulatory bodies. https://www.federalreserve.gov/newsevents/press/bcreg/20161019a.htm
- **Private**: for example the “Sheltered Harbor” plan, unveiled by the primary groups representing US financial sector entities, intended to ensure depositors and investors that their accounts will be secure after a cyberattack. http://www.wsj.com/articles/trade-groups-adopt-plan-to-better-shield-depositors-investors-from-cyberattacks-1479841201

What is FinSAC doing about it?

FinSAC is developing a new series of crisis simulation exercises in which our usual clients (Central Bank Governors, Ministers of Finance, Financial Supervisors) have to:

- deal with the business decisions required by cyber incidents, not just with their possible consequences on the liquidity and solvency of the institutions they supervise,
- interact with unusual counterparts (in-house and external IT technicians, police, national security services, etc.)

WORLD BANK GROUP
Finance & Markets

Financial Sector Advisory Center (FinSAC)

Thank you!

aalmansi@worldbank.org

www.worldbankgroup.org/finsac

Praterstraße 31 - 19 Floor, 1020 Vienna, Austria