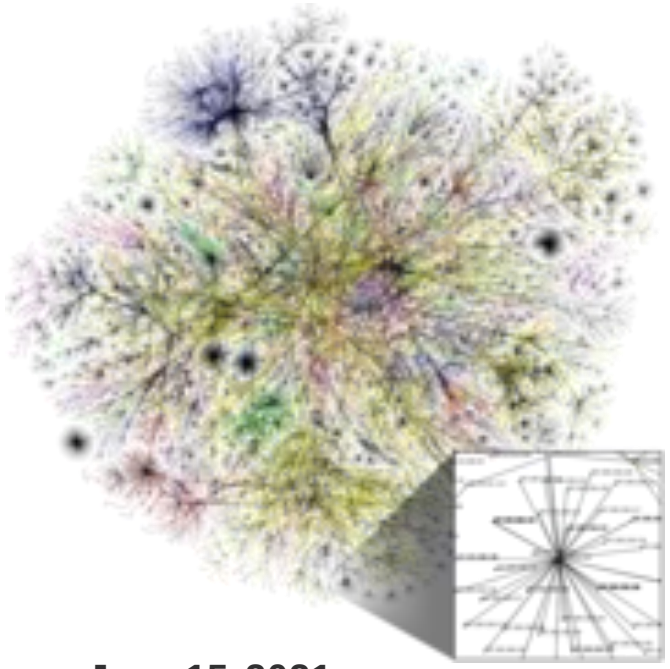
Crisis Simulation Exercises (CSEs)
National Bank of Georgia



June 15, 2021

David Papuashvili
Deputy Head
Specialized Risk Department – National Bank of Georgia
(David.Papuashvili@nbg.ge)

Disclaimer: The opinions expressed in this presentation represent those of the author and do not necessarily reflect the official position of the National Bank of Georgia.

Background

- Crisis simulation exercises (CSEs) are an important aspect of preparedness
- On August 8, 2008, distributed denial-of-service (DDoS) attacks began to affect Georgian government and commercial websites when the Beijing Olympic Games were about to commence.
- Cyber-attacks coincided (went in parallel) with the actual Russo-Georgian War on the ground.
- Denial of service attacks targeted Public, Media, Banking and Finance, Telecommunications and Energy sectors of Georgia

Effects on the Banking System

- In addition to DDoS, hackers also targeted the central bank's (NBG) website, modifying the official exchange rate that was published for the specified date.
- As a precaution, many Georgian banks disconnected their servers from the Internet.
  - Result: most bank clients were blocked from accessing essential financial services.
  - Online banking services were, in effect, offline for about 10 days.
- Main fiber optic cable connecting Eastern and Western Georgia was damaged during the invasion.
  - Banks faced communication problems and system disruptions
- At the time of the attacks, there was no dedicated unit for the supervision of operational risk within the banking system.
- Events demonstrated the need to conduct crisis simulation exercises

Crisis Simulation Exercises in the Georgian Financial System

- Started simulation exercises in 2017
- Jointly conducted with the World Bank
- Tabletop exercises
  - Do not physically impact financial institutions' information systems
- All communication is conducted electronically
- Cover cyber-risk
- Includes both the private and the public sectors

Impact of Crisis Simulation Exercises on Financial Supervision

- Increased awareness about cybersecurity within the NBG
- Speeded up the development and introduction of cybersecurity supervisory framework
- Indirectly led to the creation of a new cyber-risk supervisory unit within NBG
  - Branched off from the operational risk division
- Improved situational awareness of financial institutions about information technology-related incidents

NBG’s Cyber Risk Supervisory Framework

- Based mostly on NIST
- Key Requirements
  - Trainings (for employees) once per year
  - Management obliged to regularly check efficiency of cyber security / information security program
  - Risk and control self-assessment
  - Audit requirements
  - Penetration testing requirements
  - Incident response and recovery

Key Observations

- Simulation exercises never fully mimic reality, but are very valuable.
- Allow players to rehearse beforehand what an actual event may lead to.
- Good mechanism to test incident response.
- Financial institutions have used past experience from the exercise in real-life scenarios.
- Can also be important for decision-making associated with the recovery of operations.

Potential Outcomes of Cyber Crisis Simulation Exercises

- Cyber risk awareness
- Practice decision-making skills
- Understand the severity of the impact of a potential cyber-incident
- Crisis Management

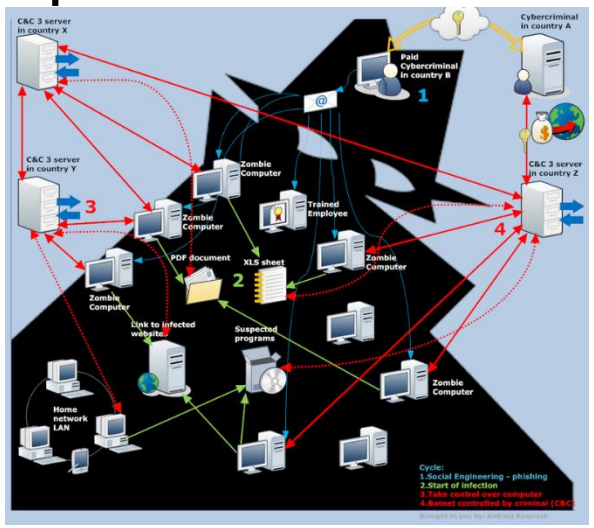
Points for Consideration

- No blame should be placed on any of the participants for their actions
  - Any failings are a result of the organization's inappropriate training
- Exercises should be close to reality
  - Create scenarios that are realistic
  - Involve people with the relevant experience for sector-specific and other forms of simulations
- Should also involve wide-ranging, and potentially unrealistic scenarios as well
  - Keep everyone involved
- All of the players should act based on actual policies and procedures.

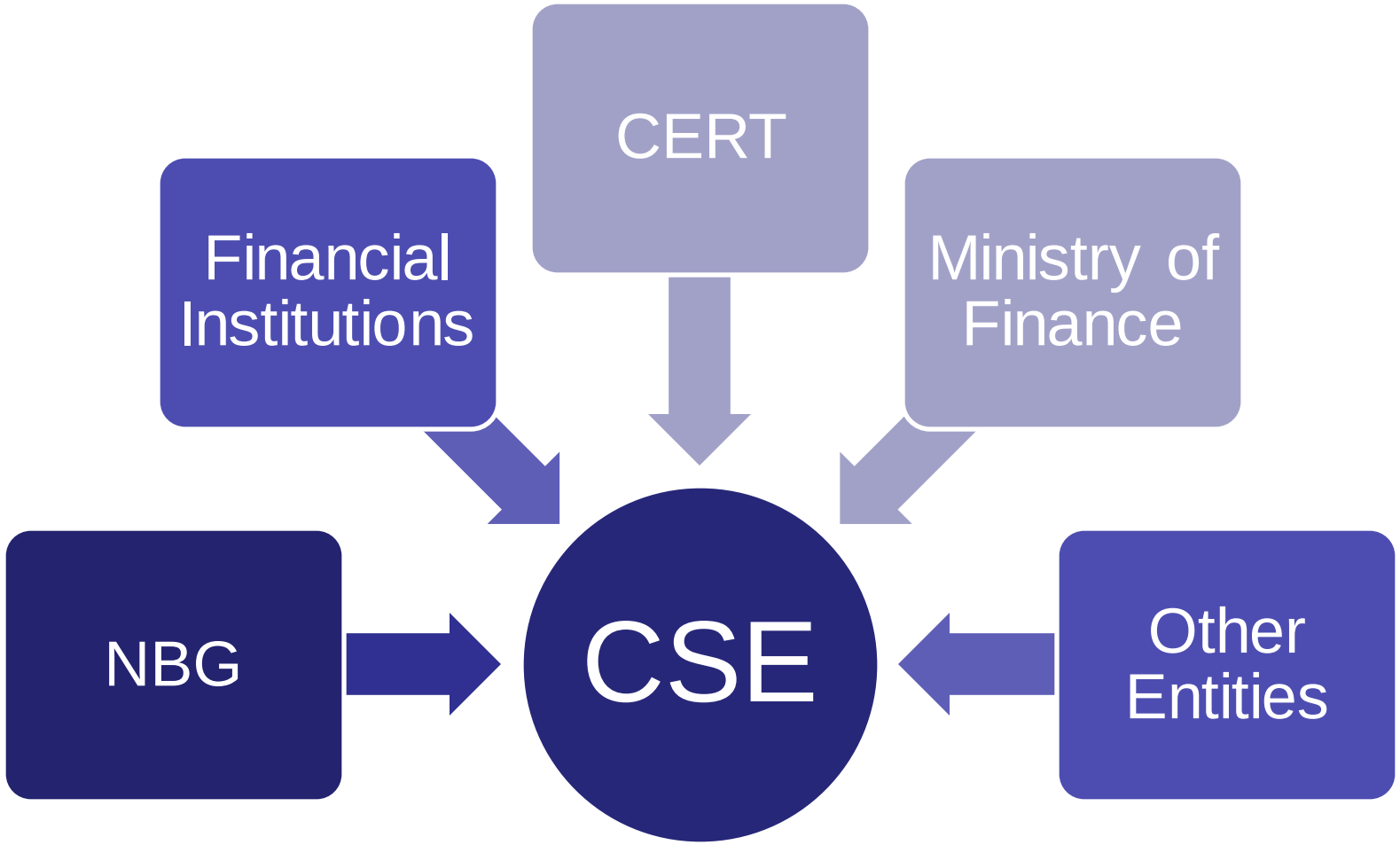
Source: Curry and Drage, 2020 and the American national Cyber Storm Exercise Guidelines

Description of the Exercises

- Exercise Type: Tabletop/Cyber Committee Game
  - Role-playing
- Scope: Sector-specific (i.e. finance)
- Number of Teams: 4-8 primary roles
- Duration of the Exercise: Around 5 hours
- Information systems are not physically impacted



Possible Primary Roles Involved



Sample Roles within the Central Bank

- Board of Governors
- Supervision
- Payment Systems
- Information Technology
- Public Relations

Potential Scenarios to Consider

- Denial of Service (including DDoS)
- Ransomware
- Insider Threat
- Unauthorized Money Transfers
- Settlement and clearing system disruptions
- Combination of the scenarios above

Lessons Learned

- To make the game effective, involve as many realistic stakeholders as possible
- Identify the critical dependencies between the financial and other sectors.
- Pre-plan the details
  - Make sure to get the names of all stakeholders right
  - Communication is key during the exercise
- Do not extend the duration of games beyond what is needed
  - **Do not make the games too long.**

Further Reading

- Lee, Y. C. Crisis Simulation Exercises. Retrieved from https://www.itu.int/en/ITU-T/extcoop/figisymposium/2019/Documents/Presentations/Yejin_C_Lee_Presentation.pdf
- Curry, J., & Drage, N. (2020). The Handbook of Cyber Wargames: Wargaming the 21st Century. The History of Wargaming Project.