Financial Sector Cybersecurity and the Pandemic

September 16, 2020 - StrategEast State and IT Eurasian Forum

David Papuashvili

Deputy Head, Specialized Risk Department

National Bank of Georgia

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.

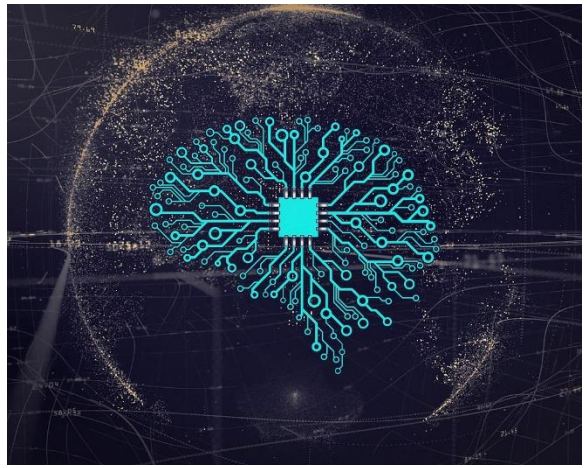
Overview

- **Cyber-risk is a systemic operational risk**
  - Can have an impact on financial stability
- Financial sector critically dependent on other sectors of the economy
  - IT
  - Telecommunications sector
  - Communication between different sectors and regulators is key
- Georgian banks increasingly using digital technologies
- FinTech becoming more widespread
  - Remote Identification
- Greater use of cloud services

Regulatory Background

- NBG Introduced operational risk requirements in 2014
  - Regulation for commercial banks
  - Covers information technology and information security
- Cybersecurity regulation adopted in 2019
  - Mandatory for commercial banks
  - Based on NIST
  - Also includes SWIFT CSP controls

Recent Developments: NBG



- Creation of a FinTech Department
- RegLab
- Increased emphasis on financial technology, digital transformation and cyber-risk
  - Report automation
- Digital Banking licenses

Board and Senior Management Involvement

- cybersecurity regulation

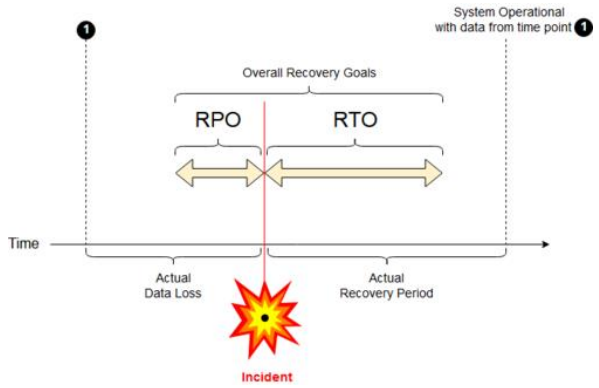
  Banks Must Conduct:

  - Trainings once per year
  - Efficiency assessment of cybersecurity program
  - Audits (information systems)
  - Penetration tests

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes
	Maintenance
	Protective Technologies
Detect	Anomalies and Events
	Security Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recovery	Recovery Planning
	Improvements
	Communications

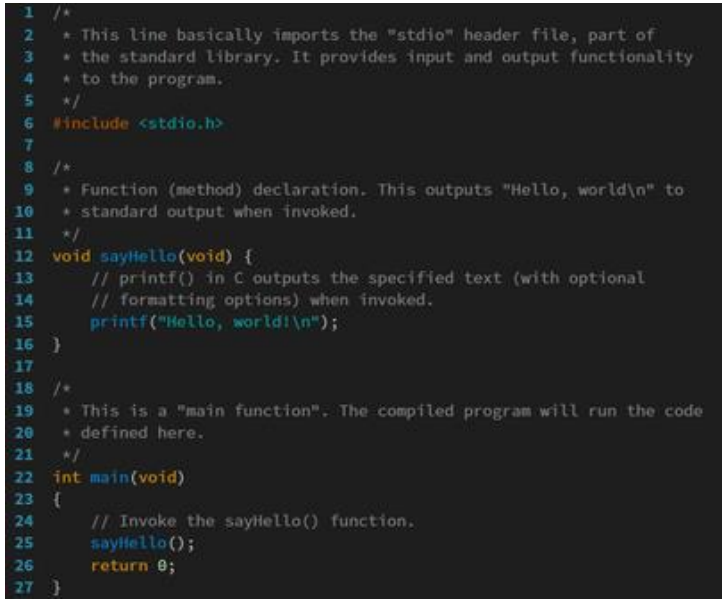
Key Aspects that the NBG Looks At

- Process Review
  - new services and systems
- Is the process adequate?
  - Design and implementation flaws
  - Use of third party technology
    - Cloud computing and associated risks
- Business continuity
  - Is the process continuous?
  - What is the potential for System disruptions?



Additional Points for Consideration for New Services

- Penetration testing
- Vulnerability scanning
- Software reviews (code assessments)



```c
/*
 * This line basically imports the "stdio" header file, part of
 * the standard library. It provides input and output functionality
 * to the program.
 */
#include <stdio.h>

/*
 * Function (method) declaration. This outputs "Hello, world\n" to
 * standard output when invoked.
 */
void sayHello(void) {
    // printf() in C outputs the specified text (with optional
    // formatting options) when invoked.
    printf("Hello, world!\n");
}

/*
 * This is a "main function". The compiled program will run the code
 * defined here.
 */
int main(void)
{
    // Invoke the sayHello() function.
    sayHello();
    return 0;
}
```

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank


Thank you