When Balance is Achieved

Digitalisation in the energy sector of Georgia – status quo, challenges and future developments

Georgi Shengelia

Minsk, 2019

Cybersecurity Development In Georgia

- Real Risks and threats experienced by Georgia in 2008
  - Wide-spread Cyber Attacks
    - website of the Georgian president & Parliament of Georgia were targeted;
    - Explosion of Baku-Tbilisi-Ceyhan gas pipeline;
    - Georgia's Internet traffic reportedly had been rerouted through servers based in other countries
  - Paralyzed critical information systems

Legal Framework regarding Cybersecurity (1)

Law on Information Security enacted in 2012 July 1st aims to

- Maintain information security
- Define rights/responsibilities for public/private sectors in the field of information security;
- Identify mechanisms for state control.

The Law defines functions of two entities:

- Cyber Security Bureau (CSB)
- Data Exchange Agency (DEA)
  - Computer Emergency Response Team (CERT)

Legal Framework regarding Cybersecurity (2)

Cybersecurity Strategy and Action Plan 2017-2018 Resolution of Government of Georgia adopted on 13th January 2017

Key Objectives and Principles:

- Cybersecurity as the integral part of the national security;
- Uncompromised protection and respect for the human rights and basic freedoms;
- Common approach of the Government of Georgia;
- Collaboration between the state and private sectors;
- Active international cooperation;
- Individual responsibility;
- Adequate measures.

Data Exchange Agency

- Data Exchange Agency main functions
  - Develop state policy for e-governance
  - Ensure information security
  - Monitor the unified government network
  - Develop information technologies/systems and relevant standards
  - Pre- and Post-Implementation Reviews
  - Provide Audit IT Systems
  - Advisory on planning Information Security
  - Establish and coordinate CERT
- Critical Information System Subjects are required to follow ISO 27001 standard

Gaps In the Regulation

- The list of “Critical Information System Subjects” is approved by Government of Georgia
- Utilities and Energy Generators are not included in the **list**
- GNERC is not authorized to develop Cybersecurity Strategy **by Law**

Draft Cybersecurity Strategy

1. Strategy Defines Goals of the GNERC
2. Utilities and Generators with remote automated control systems are included in the list.
3. Strategy requires to make investments in cybersecurity and satisfy minimum standards
4. Strategy lists the main stakeholders: Government organizations and Public sector
5. Standards are adopted according to Information Security Law
6. Working Group is defined to monitor cybersecurity progress of regulated entities

Fulfilment of Action Plan

- **Questionnaire with approximately 200 questions was sent to regulated entities in September 2018**
- **Working Group together with DEA analyzed answers and reported results to Commission;**
- **General meeting with companies was held on November 7th, 2018**
  - Companies were instructed to define person/persons who will be responsible for monitoring cybersecurity issues within the company and reporting to the Commission
  - Companies were asked to define what standards or solutions are most relevant for them and provide their suggestions or visions to the commission

Recent Developments and Future Plans

Recent Developments

- **DEA will develop cybersecurity standards for every sector including energy**
- **At this point GNERC, other regulators and DEA are cooperating to develop:**
  - New Cybersecurity Strategy for Georgia
  - Appropriate Amendments to Laws

Future Plans

- Define sector specific standards
- Define evaluation tools
- Establishment of the cybersecurity working group.

GNERC

when balance is achieved

#whenbalanceisachieved

Georgi Shengelia
Deputy Director of International Relations' Department, GNERC
g.shengelia@gnerc.org