CYBER SECURITY

Lessons from World Bank Projects

WORLD BANK GROUP

Anat Lewin
Senior ICT Policy Specialist
alewin@worldbank.org

Energy Grids and Water Utilities are Vulnerable

- **Energy:** In the Ukraine in December 2015, hackers struck three electric distribution centers, leaving 230,000 people in the dark and cold, and flooded call centers with bogus calls that hampered detection and recovery efforts.

- **Water:** Hackers breached an unidentified water utility and manipulated systems responsible for water treatment and flow control, Verizon said in a report released March 2016. Investigators believe the hackers exploited a vulnerability in the payment application web server. Attackers are believed to have stolen 2.5 million records containing customer and payment information. The system also ran valve and flow control applications; the hackers managed to access this software and alter settings related to water flow and the amount of chemicals used to treat the water.

- **Central Government**: Hack against US Office of Personnel Management in 2014 compromised personal data of 21.5 million people.

Bangladesh Case

- In February 2016, the central bank of Bangladesh lost $81 million due to a cybersecurity attack.
- Skilled cybercriminals issued 35 instructions using the SWIFT messaging system used by banks that amounted to $951 million in transfers to casinos in the Philippines, Sri Lanka and other countries.
- Fortunately, most of the transfers were blocked before they could be made.
- However, Bangladesh, a lower middle income country with a poverty headcount of 31.5% and a per capita GNI of $1080, suffered a loss of $81 million that will likely need to be covered from its central bank reserves.
- The funds remain missing.
- In May 2016, Tien Phong Bank in Vietnam announced that it thwarted an attack on its banking system in Q4 of 2015 that used a similar technique to the one in Bangladesh.

How the World Bank is Supporting Bangladesh

- Establishing information security program, goals, priorities.
- Setting up the first CIRT in the country to:
  - Serve as a focal point of contact and coordination within and beyond national border;
  - Identify and manage cyber threats that may have adverse affect on the country;
  - Help systematically respond to cyber security incidents and takes appropriate actions;
  - Help the constituency to recover quickly and efficiently from security incidents;
  - Minimize loss or theft of information and disruption of services;
  - Establish and nurture relationships with other international/regional CIRTs;
  - Make security best practices and guidance available through publications, websites;
  - Participate in initiatives (or set directions and drive the projects) pertaining to developing national policies, strategies, laws and regulations for cyber security;
  - Provide trainings to improve the skill-sets, competency, confidence of CIRT personnel;
  - Improve the readiness, availability and reliability of ICT infrastructure and services to the public as well as the private sector;
  - Develop and implement cyber security awareness campaigns to the general public;
  - Develop a sound financial plan and operational plan for its own sustainability.

Bhutan Assistance

- The Bank funded a CIRT implementation in Bhutan
- The support included capacity building on policy and regulatory issues
- The CIRT was implemented by a multi-stakeholder team that included the private sector and was coordinated by Department of IT and Technology (DITT)
- The Bank in association of Oxford University team also completed a cyber security assessment for Bhutan

Cyber Security Maturity Assessment In Collaboration with Oxford University

- Partnership with Global Cyber Security Capacity Centre (GCSCC) at Oxford.
- GCSCC created a model to measure cybersecurity maturity across five dimensions.
- Model enables nations to self-assess, benchmark, better plan investments and national cybersecurity strategies, and set priorities for capacity development.
- Dimensions are
  - Devising cyber policy and strategy
  - Encouraging responsible cyber culture within society
  - Building cyber skills into the workforce and leadership
  - Creating effective legal and regulatory frameworks
  - Controlling risks through organization, standards and technology
- Delivered to Armenia, Kosovo and Bhutan

Global Cyber Security Capacity Centre

Building Cyber-security Capacity in the Republic of Armenia

https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf

What Best Practice Countries Are Saying

- No threat is unique, no attack is unique. What happens in one country will happen in another country, Information sharing is key.
- Be very selective when identifying critical infrastructure – if everything is critical, nothing is critical.
- Assume that hackers can eventually penetrate and one needs to focus on detection, limitation, mitigation and damage control.
- With limited resources, trust and close collaboration between public sector, private sector and academia are essential to success.
- Championship and awareness of Decision Makers at high governmental levels is needed.
- Cyber education could start in secondary schools as part of formal courses in cyber security, computer programming, and Internet ethics. Teaching Internet ethics is intended to avoid youth to become hackers.
- A computer that isn’t attached to a network still needs to be secured physically.
- Government should strongly incentivize R&D and provide resources for it.

WORLD BANK GROUP

What Our Client Countries' Cyber Policy Officials Are Saying

- Prioritize strengthening national CERTs, CIRTS, SOCs and critical sector versions of them.
- Need to place more government focus on protecting critical infrastructures such as energy, water and banking.
- Need to develop highly-skilled, strong cyber security workforce and create a cyber-aware, cyber-active culture. Capacity building is key.
- Want to develop local Cyber capacity building training labs.
- Need to develop an efficient collaborative model between government organizations, the business community and the academia for the advancement of national cyber security. PPP Community Building.
- Need to raise Cyber awareness of non-technical government officials at all levels.

The Future: Internet of Things

- CISCO White Paper estimated that 50 billion devices will be connected to the Internet by 2020.
- HP report states that 70 percent of IoT devices contain serious vulnerabilities.
- As more devices are connected to the Internet, the need for Cyber Security becomes more crucial. E.g.:
    - Driverless cars
    - Biomedical devices (implants)
    - Smart homes
    - Wearables (fitness trackers)

http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

WORLD BANK GROUP

We must act together

- Cyber threats against government systems worldwide are growing in number.
- Because groups of organized cyber attackers can use the same techniques in different countries and an attack on one government can be repeated in another country, it is important for governments to share information and best practices in responding to those attacks.

“We cannot solve cybersecurity in isolation. The whole universe is one family. If something happens in one country, it is not just their problem. We have to build a coalition.”

J.A. Chowdary, IT Advisor to the Chief Minister of Andhra Pradesh, India.

World Bank Cyber Security Projects

- The World Bank is offering integrated solutions in the ICT project portfolio **to address cybersecurity gaps** in our country clients.

- We have different projects in which we are trying to increase countries’ response capacity to cyber-threats menacing their public systems and infrastructure, especially those projects that have eGovernement, eservices, eIDs, Open Data, among other components.

Lending

ECA REGION:
***Armenia**
***Moldova**

AFRICA REGION:
***Uganda**
***Tanzania**
***Rwanda**
***Benin**
***Comoros**
***Mozambique**
***E-Ghana**
***E-Kenya**

EAP REGION:
***Myanmar**

Technical Assistance

SOUTH ASIA:
***Bhutan**

ECA REGION:
***Montenegro**
***Kosovo**

WORLD BANK GROUP
Transport & ICT

THANK YOU

WORLD BANK GROUP

Anat Lewin
Senior ICT Policy Specialist
alewin@worldbank.org
Linkedin.com/anatlewin