ECA REGIONAL CYBER-SECURITY ISSUES AND OPTIONS (BASED ON A 14 COUNTRY SURVEY)

PART I: CYBER-THREATS

FERNANDO MONTES-NEGRET
FINSAAC COORDINATOR, THE WORLD BANK
MAY 18TH, 2015
A Positive Message:  
Finance has contributed significantly to economic progress

“TECHNOLOGICAL PROGRESS IN FINANCIAL SERVICES HAS PLAYED A CRUCIAL ROLE IN MAKING THE SYSTEM WORK EFFICIENTLY, ENABLING GREATER AUTOMATION PROCESSES, HIGHER PROCESSING POWER, IMPROVED RISK MANAGEMENT AND A WIDER PRODUCT RANGE AVAILABLE ON ONLINE PLATFORMS. THIS BENEFITS BUSINESS AND RETAIL CUSTOMERS”.

Inconsistencies: Information and the Regulatory Perimeter

- Central Bank
- NBFIs (Regulated/Lightly Regulated)
- Non-Financial Institutions (non-Reporting/Unregulated)
- Other (Non-Reporting/Unregulated)
Cyber-Threats & Vulnerabilities

Software
Old, more vulnerable, IT legacy systems;
Merged IT systems, not always fully compatible;
Use of internal & external resources to manage IT systems;
Phishing and malware;
Crypto-locker blackmail;
Wiper hacks;
Advanced persistent threats;

Access
Vulnerabilities of the two-step verification software;
Weak passwords and lax access policies;
No or weak oversight over third party service providers and vendors’ systems & controls (outsourcing);
Cyber-Threats & Vulnerabilities (cont. 2)

**Employees, Third Party Vendors & Outsourcing**
Staff stealing in-house proprietary and confidential information;
Cross-border crime difficult to police & punish;
Independent and State-backed hackers;
Launching of new, untested, products;
Excessive reliance on third-party service providers for critical banking functions, including payment processing, web applications, and online banking;

**Targets**
Account takeovers, identity theft, telecommunication network disruptions, and data integrity breaches;
Theft of proprietary trading algorithms and other intellectual property and valuable know-how;
Customer accounts & data;
ATM and point of sale schemes and other financial infrastructure.
General Responses to Cyber Risks Information Security Framework

✓ Written information security policy;
✓ Security awareness education and employee training;
✓ Identification and management of key cyber risks and trends;
✓ Information security audits;
✓ Incident monitoring & reporting
  Ten Steps Guidance:
  a. Information Risk Management Regime;
  b. Secure Configuration;
  c. Network Security;
  d. Managing User Privileges;
  e. User Education and Awareness;
  f. Incident Management;
  g. Malware Prevention;
  h. Monitoring;
  i. Removable Media Controls; and
  j. Home & Mobile Working.
Other
✓ Strong cyber-security governance (beyond IT Departments, including a dedicated information security executive);
✓ Frequent security updates & reporting to Board of Directors and relevant managers;
✓ Adequate information security budget;
General Responses to Cyber Risks Information Security Framework (cont. 2)

Cyber-Insurance & Partnerships
✓ External insurance coverage;
✓ Information sharing among financial institutions, retailers, and security agencies (Information Sharing and Analysis Centers, in spite of reluctance to reveal security weaknesses to competitors);
✓ A more concerted response from all parties;
✓ Sharing of information in real time among trusted parties;
✓ Speedy response;

Cyber-attack Bills
✓ Sharing the losses among: banks- insurers- retailers;
✓ Setting industry data protection standards (Gramm-Leach-Bliley Act in the US);

Software
✓ Anti-virus software and (internet) firewalls;
✓ Detection of unauthorized devices;
✓ Spyware and malware detection;
✓ Server-based access control lists;
✓ Intrusion detection tools & intrusion prevention systems;
General Responses to Cyber Risks Information Security Framework (cont. 3)

Training of bank staff
✓ Vulnerability scans and (internal 7 external) penetration tests;
✓ Encryption: files and information traffic;
✓ Data loss prevention tools;
✓ Make software providers liable for vulnerabilities;
✓ More effective passwords and access codes (multi-factor authentication & encryption);
✓ Smart cards and one-time password tokens;
✓ Biometric tools;
  Communication Strategy
✓ Communication plan & designated communication officer following a cyber-security breach.
  Supervisory Actions
✓ More frequent and detailed IT examination procedures focused on cyber security;
✓ Review of IT governance arrangements, response and event management;
✓ More focus on internal access controls and security;
✓ Review of contracts for Vendors, screening compliance with management policies;
✓ Disaster recovery plans and enforcement legislation
✓ Require regular reporting of cyber-attacks to supervisor
Cyber-Preparedness is a Policy Issue: Main Messages

Cyber-Preparedness is a Policy Issue, with an important IT component, but it is not only an IT issue;

Governance of cyber-risks is paramount, at: CBs & Regulatory Agencies, Banks and Non-Bank Financial Institutions, FMIs, and private & public corporations;

It reflects the pervasive nature of information, which extends to all players in the economy holding private/confidential client information;

Role of Central Banks & Supervisory Agencies, Consumer Protection Agencies, Security Services;

Bank’s Boards and Bank Supervisors have a key role to play. They need better intelligence, be more pro-active to confront, prepare and invest to contain cyber-risks;

Ask your technical staff the hard questions!. Frankly you need to think “out of the box”!

It is likely that a future systemic crisis might have a significant cyber-event.

A dynamic and complex process, requiring the coordination of multiple stakeholders.

⇒ Need to prepare, be alert and invest. No time for complacency;
⇒ The economic and non-economic costs of cyber-attacks are on the rise!.
# Reducing the cyber risk in 10 critical areas

<table>
<thead>
<tr>
<th>Information Risk Management Regime</th>
<th>Secure Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a governance framework: Enable and support risk management across the organisation.</td>
<td>Develop systems to update and patch systems: Establish and maintain policies that set out the procedures for applying updates and patches.</td>
</tr>
<tr>
<td>Determine your risk appetite: Decide on the level of risk the organisation is prepared to tolerate and communicate it.</td>
<td>Create and maintain hardware and software inventories.</td>
</tr>
<tr>
<td>Maintain the Board’s engagement with cyber risk: Make cyber risk a regular agenda item. Record cyber risks in the corporate risk register to ensure senior ownership.</td>
<td>Use automated tools to create and maintain inventories of every device and application used by the organisation.</td>
</tr>
<tr>
<td>Produce supporting risk management policies: An overarching corporate security policy should be produced together with an information risk management policy.</td>
<td>Leak a baseline security build for workstations, servers, firewalls and any other software.</td>
</tr>
<tr>
<td>Adopt a lifecycle approach: Risk management is a whole life process and the organisation’s policies and processes should support and enable this.</td>
<td>Conduct regular vulnerability scans: Run automated vulnerability scanning tools against all networked devices at least weekly and remedy any vulnerability within an agreed time frame.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Security</th>
<th>Managing User Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Police the network perimeter: Establish multi-layered boundary defences with firewalls and proxies deployed between the untrusted external network and the trusted internal network.</td>
<td>Establish effective account management processes: Manage and review user accounts from creation and modification to eventual deletion.</td>
</tr>
<tr>
<td>Protect the internal network: Prevent any direct connections to external services and protect internal IP addresses.</td>
<td>Limit the number and use of privileged accounts: Minimise privileges for all users. Provide administrators with normal accounts for business use. Review the requirement for a privileged account more frequently than standard accounts.</td>
</tr>
<tr>
<td>Monitor: Use intrusion monitoring tools and regularly audit activity logs.</td>
<td>Monitor all users: Monitor user activity, particularly access to sensitive information and the use of privileged accounts.</td>
</tr>
<tr>
<td>Test the security controls: Conduct regular penetration tests and undertake simulated cyber attack exercises.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Education and Awareness</th>
<th>Incident Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Produce a user security policy: Produce policies covering the acceptable and secure use of the organisation’s systems.</td>
<td>Obtain senior management approval and backing: The Board should lead on the delivery of the incident management plans.</td>
</tr>
<tr>
<td>Establish a staff induction process: New users should receive training on their personal security responsibilities.</td>
<td>Establish an incident response and disaster recovery capability: Develop and maintain incident management plans with clear roles and responsibilities, regularly test your plans.</td>
</tr>
<tr>
<td>Maintain user awareness of the threats: All users should receive regular refresher training on the cyber risks to the organisation.</td>
<td>Provide specialist training: The incident response team should receive specialist training to ensure they have the skills and expertise to address the range of incidents that may occur.</td>
</tr>
<tr>
<td>Support the formal assessment of IA skills: Encourage relevant staff to develop and formally validate their IA Skills.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Malware Prevention</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop and publish corporate policies: Produce policies to manage the risks to the business processes from malware.</td>
<td>Establish a monitoring strategy and supporting policies: Implement an organisational monitoring strategy and policy based on an assessment of the risks.</td>
</tr>
<tr>
<td>Establish anti malware defences across the organisation: Agree a corporate approach to managing the risks from malware for each business area.</td>
<td>Monitor all networks and host systems (e.g. clients and servers).</td>
</tr>
<tr>
<td>Scan for malware across the organisation: Protect all host and client machines with anti virus solutions that will automatically scan for malware.</td>
<td>Monitor network traffic: Network traffic should be configured to identify unusual activity or trends that could indicate an attack.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Removable Media Controls</th>
<th>Home and Mobile Working</th>
</tr>
</thead>
<tbody>
<tr>
<td>Produce a corporate policy: Implement policy to control the use of removable media for the import and export of data.</td>
<td>Assess the risks and create a mobile working policy: The policy should cover aspects such as information types, user credentials, devices, encryption and incident reporting.</td>
</tr>
<tr>
<td>Limit the use of removable media: Limit the media types that can be used together with user and system access and the information types that can be stored on removable media.</td>
<td>Educate users about the risks and train them to use their mobile device securely by following the security procedures.</td>
</tr>
<tr>
<td>Scan all removable media for malware: All clients and systems should automatically scan removable media. Any media brought into the organisation should be scanned for malware by a stand alone scanner before any data transfer takes place.</td>
<td>Apply the secure baseline build: All mobile devices should be configured to an agreed secure baseline build. Data should be protected in transit and at rest.</td>
</tr>
</tbody>
</table>