Cybersecurity in Credit Reporting

November 2019
OUTLINE

• Background

• Survey
  • Respondents
  • Survey findings
  • Policy considerations

• Suggested way forward
BACKGROUND

• Changes in credit reporting industry landscape including the adoption of new technologies and business models and the emergence of new players posing additional risks for CRSPs.

• Several CRSPs have been subject to data breaches, denial-of-service attacks, and phishing attacks, among other cyber incidents in the past decade resulting in financial, economic, operational, and reputational loss.

• Against this background, the ICCR drafted Guidelines on the Cybersecurity in Credit Reporting building on General Principles on Credit Reporting.

• This guideline provides findings of a landscaping survey conducted by the Committee on CRSPs across the globe on current practices and proffers some policy considerations.
Data Processing: Security and Efficiency
GP 2: Credit reporting systems should have rigorous standards of security and reliability, and be efficient.

Governance and Risk Management
GP3: The governance arrangements of CRSP and data providers should ensure accountability, transparency and effectiveness in managing the risks associated with the business and fair access to the information by users.

Recommendation E: Central Banks, Financial supervisors, and other relevant authorities, both domestic and international should cooperate with each other, as appropriate in promoting the safety and efficiency on credit reporting systems.
Survey:
### Response Statistics

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Responses</td>
<td>45</td>
</tr>
<tr>
<td>Completion Rate</td>
<td>85%</td>
</tr>
<tr>
<td>Exclusions</td>
<td>10</td>
</tr>
<tr>
<td>Number Analyzed</td>
<td>35</td>
</tr>
</tbody>
</table>

- 7 - Incomplete Responses
- 3 - Duplications
Respondents Demographics

**Respondents by Organization Type**
- Private: 30
- Public: 5

**Geographical Dispersion of Respondents**
- Africa: 43%
- Americas: 23%
- Asia: 17%
- Europe: 14%
- Middle East: 3%
## Survey Topics

- Local cybersecurity environment
- Legal and regulatory environment
- Board, Management and Cybersecurity and Information Security Strategy
- Outsourcing Critical IT services
- Information Sharing
- Training and Awareness
- Resources
- Risk Management and compliance
- Audit
- Incident response
- Data loss prevention
- Preventive controls
Cybersecurity incidents Q5-13

- **Attack to others**
  - 6 data breaches
  - 3 unauthorized access
  - 2 DoS & DDoS
  - 1 undisclosed
  - 2 other

- **Attack to data providers**
  - 3 data breaches
  - 3 unauthorized access
  - 1 ransomware
  - 3 other

- **Cyber attacks to the institution**
  - 5 DoS & DDoS
  - 1 unauthorized access
  - 1 phishing
  - 1 other
Legal and regulatory environment Q14-19

- Laws on cyber?
- Obligation to compensate?
- Obligation to notify affected?
- Obligation to report incident?
- Penalties?

Bars indicate percentage of responses:
- Yes
- No
- N/A
<table>
<thead>
<tr>
<th>Question</th>
<th>Yes (%)</th>
<th>No (%)</th>
<th>N/A (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breaches are communicated?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Institution is insured?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy includes insurance coverage?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strategy includes outsourcing?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employees accountable?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber senior independent?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber senior report to CEO or board?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policies include roles and is comm?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The board engages experts?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A director cyber savvy?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board understand cyber controls?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board reviews strat when there is a...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board approves strategy?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a Cyber strategy?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Most senior Cyber officer**
- 17 CIO
- 14 CISO
- 1 CEO
- 1 General counsel
- 1 VP
- 1 CRO
Outsourcing Critical IT services Q35-37

Cyber policies set controls for third parties?
- yes
- no
- N/A

The institution outsources Critical services

- Cloud
- Network and Security
- Data Centres
- Other
Information Sharing Q38-40

- The institution receives notification of cyber incidents from vendors?
- Cyber team monitors industry incidents and participates in industry programs?
- Cyber team engages in information sharing?

Graph showing responses: yes, no, and N/A.
Training and Awareness Q41-45

- Training includes incidence response and new trends?
- Employees with privileged access permissions receive training on...
- Cyber training to managers on their roles?
- Cyber training for the BOD last 12 months?
- Cyber awareness training program?

![Bar chart showing percentages of yes, no, and N/A responses]
Is investment on cyber adequate to the risk?

Is Cyber incidents discussed and estimated in the budget process?

Is there budget for Cyber?
Risk Management and compliance Q49-51

The institution complies with data privacy regulations? [Blue]

Risk management function assessment of the framework is commensurate to the risk? [Blue]

Risk management framework includes Cyber risk? [Blue]

- [Blue] yes
- [Orange] no
- [Gray] N/A
Audit Q52- 56

Audit validates that incident response program is adequate to risk and complexity

Audit validates that the third party mgmt is adequate to risk and complexity

Audit validates that the cyber controls are adequate to risk and complexity

Audit validates that the threat information sharing is adequate to risk and complexity

Internal audit unit has resources and expertise to audit cyber

yes no N/A
Incident Response Q57-63

- Incident response simulation exercise?
- The institution partners with CERT?
- External communications plan for cyber incidents?
- Internal communication plan for Cyber incidents?
- Process to escalate to srn mngmt on breaches based on thresholds?
- Dedicated security incident team to respond to incidents?
- Documented process to monitor, analyze and respond to incidents?

- yes
- no
- N/A
### Data Loss Prevention Q64-68

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes (%)</th>
<th>No (%)</th>
<th>N/A (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there rules to control printing sensitive docs and info?</td>
<td>60</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>DLP rules are in place to identify, block or encrypt data</td>
<td>65</td>
<td>30</td>
<td>5</td>
</tr>
<tr>
<td>Processes to capture DLP events are in place?</td>
<td>68</td>
<td>29</td>
<td>3</td>
</tr>
<tr>
<td>The institution require user verification prior to sending mail?</td>
<td>67</td>
<td>30</td>
<td>3</td>
</tr>
<tr>
<td>DLP program and WSO to monitor and prevent breaches?</td>
<td>60</td>
<td>35</td>
<td>5</td>
</tr>
</tbody>
</table>
Preventive Controls Q69- 79

- Physical controls for data center access?
- Vulnerability scans on SW and HW are regular?
- Automated process to detect and block changes to SW and HW?
- Change management process?
- Security configuration standards to HW and SW?
- Is there an inventory of technology assets?
- Are there strong authentication mechanisms?
- Are there tight controls for admin privileges?
- Remote access policies for internal resources over public network?
- Is unauthorized network access automatically detected and blocked?
- Is the network segmented in separate trust zones?

- yes
- no
- N/A

*Percentage distribution:*

- 0% 20% 40% 60% 80% 100%
POLICY CONSIDERATIONS

• Authorities need to consider:

  • Implementing and/or enhancing cyber laws and regulations.
  • Developing national and/or sector-wide cybersecurity strategies and frameworks.
  • Implementing practices or standards that promote the strengthening of cyber governance by CRSPs.
  • Requiring CRSPs to develop detailed programs for training their boards of directors.
  • Issue guidance on the level and extent of disclosures of security and data breaches.
  • Ensure that CRSPs implement sound outsourcing procedures that detail the controls and processes to be followed when evaluating and managing relationships with third parties.

• Subjecting third parties that service CRSPs with the same level of risk management practices expected of the entities themselves.
POLICY CONSIDERATIONS

• Conducting annual cybersecurity risk assessments of critical infrastructure players.

• Encouraging CRSPs to conduct their own internal assessments on a periodic basis.

• Promoting regular cyber audits of cyber functions.

• Developing mechanisms that foster and enforce cyber information sharing and collaboration among parties.

• Publishing or promote publication of redacted reports on cybersecurity issues on a semi-annually (half yearly) basis.

• Ensuring that CRSPs actively participate and collaborate with national cybersecurity actors such as CERTs.
SUGGESTED WAY FORWARD

• The Committee will be working on:
  • dissemination of the guideline through workshops.
  • participating in the development of assessment toolkit.
  • conducting country assessments with a view of promoting technical assistance.
  • administering periodic surveys of state of cybersecurity.