Approaches and Practices for Increasing Maturity and Capabilities for CSIRTs in Emerging Economies

Jean-Robert Hountomey, Unal Tatar, Sherif Hashem, Kaleem Ahmed Usmani, Hayretdin Bahsi

March 2, 2022
Project Goal

This project aims to create a tailorable guide for emerging economies to develop or improve their CSIRT capabilities in an affordable way to respond to the evolving cyber threat environment effectively.
Methodology

- Desk review
- Data collection and analysis
  - Surveys
  - Interviews
- Validation
Project Reports
Part 1:
Literature review
Literature Review

- Maturity models
- N-CSIRT guidelines and best practices
- Tools
- Trainings
- Legal frameworks
- Specific national practices
Part 2:
Current state and future projection of N-CSIRTs in emerging economies
Results of Survey & Interviews
Survey

• Conducted a survey to understand which services those CSIRTs deliver, what type of technical and organizational capabilities they have, what their medium- and long-term goals, and their best practices in capacity building.

• The findings of the desk review were utilized for identifying the objectives and questions of the survey of low-income N-CSIRTs.

• 28 respondents representing N-CSIRTs participated in the survey, but incomplete or repetitive submission were excluded, resulting in 16 final responses.
<table>
<thead>
<tr>
<th>Country</th>
<th>Region</th>
<th>GDP Per Capita</th>
<th>Human Development Index Ranking</th>
<th>Global Cybersecurity Index Ranking</th>
<th>Digital Development Level</th>
<th>Which year was your B-CERT launched?</th>
<th>Does your nation have a national cyber security strategy?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mauritius</td>
<td>Africa</td>
<td>$22,989</td>
<td>0.804</td>
<td>17</td>
<td>60.83</td>
<td>2008</td>
<td>Yes</td>
</tr>
<tr>
<td>Egypt</td>
<td>Africa</td>
<td>$11,763</td>
<td>0.707</td>
<td>23</td>
<td>49.58</td>
<td>2009</td>
<td>Yes</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Asia Pacific</td>
<td>$11,812</td>
<td>0.718</td>
<td>24</td>
<td>50.22</td>
<td>2013</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunisia</td>
<td>Africa</td>
<td>$10,756</td>
<td>0.740</td>
<td>45</td>
<td>51.96</td>
<td>2004</td>
<td>Yes</td>
</tr>
<tr>
<td>Nigeria</td>
<td>Africa</td>
<td>$5,136</td>
<td>0.539</td>
<td>47</td>
<td>35.86</td>
<td>2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Bangladesh</td>
<td>Asia Pacific</td>
<td>$4,754</td>
<td>0.652</td>
<td>53</td>
<td>36.22</td>
<td>2015</td>
<td>Yes</td>
</tr>
<tr>
<td>Benin</td>
<td>Africa</td>
<td>$3,287</td>
<td>0.545</td>
<td>56</td>
<td>30.41</td>
<td>2017</td>
<td>Yes</td>
</tr>
<tr>
<td>Uruguay</td>
<td>Latin America/Caribbean</td>
<td>$21,561</td>
<td>0.817</td>
<td>64</td>
<td>67.94</td>
<td>2017</td>
<td>Yes</td>
</tr>
<tr>
<td>Dominican Republic</td>
<td>Latin America/Caribbean</td>
<td>$18,419</td>
<td>0.756</td>
<td>66</td>
<td>48.26</td>
<td>2018</td>
<td>Yes</td>
</tr>
<tr>
<td>Zambia</td>
<td>Africa</td>
<td>$3,479</td>
<td>0.584</td>
<td>73</td>
<td>35.56</td>
<td>2012</td>
<td>Yes</td>
</tr>
<tr>
<td>Cote d'Ivoire</td>
<td>Africa</td>
<td>$1,616</td>
<td>0.538</td>
<td>75</td>
<td>39.99</td>
<td>2009</td>
<td>Yes</td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>Asia Pacific</td>
<td>$13,078</td>
<td>0.782</td>
<td>83</td>
<td>49.55</td>
<td>2006</td>
<td>Yes</td>
</tr>
<tr>
<td>Botswana</td>
<td>Africa</td>
<td>$17,786</td>
<td>0.735</td>
<td>88</td>
<td>47.35</td>
<td>2020</td>
<td>Yes</td>
</tr>
<tr>
<td>Malawi</td>
<td>Africa</td>
<td>$1,080</td>
<td>0.483</td>
<td>97</td>
<td>27.99</td>
<td>2018</td>
<td>Yes</td>
</tr>
<tr>
<td>Togo</td>
<td>Africa</td>
<td>$1,396</td>
<td>0.535</td>
<td>105</td>
<td>N/A</td>
<td>2021</td>
<td>No</td>
</tr>
<tr>
<td>Trinidad and Tobago</td>
<td>Latin America/Caribbean</td>
<td>$26,176</td>
<td>0.796</td>
<td>123</td>
<td>59.49</td>
<td>2012</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Survey Results: General Challenges for N-CSIRTs
Survey Results: HR Challenges for N-CSIRTs

- We need more staff members to have better service quality.
- We have sufficient staff but need to increase their qualification to have better service quality.
- We have sufficient staff to fulfill our services with high quality.
- We have a significant level of staff shortage.
Survey Results: Technical Skills Needed
Survey Results: Soft Skills Needed

- Communication (written/oral)
- Relationship management at the national and international levels
- Coping with stress
- Problem-solving
- Ability to follow policies and procedures
- Teamwork
- Time management
- Presentation
- Integrity
Survey Results: Tools Needed

- Threat intelligence feeds
- Network packet capturing tools
- Digital forensics tools (e.g., imaging, analysis, and reporting)
- Vulnerability scanning tools
- Malware analysis tools
- Reverse-engineering tools
- Stakeholder management tools
- Business process management tools
- Others
Survey Results: Tool Challenges

Among the 16 N-CSIRTs:

- 13 do not have enough budget to buy high-quality tools.
- 12 use open-source tools in production environments,
  - 4 either prefer not to use or use open-source tools for testing purpose, and
  - 5 prefer open-source rather than commercial tools.
Survey Results: Trainings

• Majority do not utilize platforms like EDX, Coursera, Udemy, Udacity, Lynda, and others.

• A host of training providers exist but for the 16 N-CSIRTs:
  • FIRST, AfricaCERT, and ITU are used several times or frequently
  • Providers like OAS, CREST, LACCIRT are known by or used by a few.
  • There are existing arrangements with organizations like SANS, ISC2, COMPTIA for National level capacity building initiatives.
Interviews

• Interviews with N-CSIRTs
  • To clarify the survey responses and get a deeper view, the following N-CSIRTS were interviewed:
    • Ivory Coast CERT
    • TG-CERT
    • EG-CERT

• Interviews with Leading Experts and SMEs
  • To get insights from an external party about challenges and best practices of N-CSIRT capacity development in low-income countries
Affordable tools and trainings for N-CSIRTs

A recommendation per FIRST Services Framework
Mapping Services with Tools & Trainings

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- Information Security Incident Coordination
- Crisis Management Support

1. SERVICE AREAS
   - Information Security Incident Management
   - Monitoring and Detection
   - Event Analysis
   - Awareness Building
   - Training and Education
   - Exercises
   - Technical and Policy Advisory
   - Knowledge Transfer
   - Situational Awareness
   - Data Acquisition
   - Analysis and Synthesis
   - Communication

2. Vulnerability Management
   - Vulnerability Discovery/Research
   - Vulnerability Report Intake
   - Vulnerability Analysis
   - Vulnerability Coordination
   - Vulnerability Disclosure
   - Vulnerability Response

3. NICE - National Initiative for Cybersecurity Education

4. TOOLS + TRAINING
Innovations in N-CSIRT capacity building & Recommendations
Innovations and Recommendations (Selected)

- Creating a pipeline of cybersecurity workforce: cooperation with universities and academic institutions
- Leveraging public-private partnership to operate
- Trust building
- Knowledge transfer from other N-CSIRTs
- Funding and support through regional and international cooperation
Thank you!

- BGD e-GOV CIRT, Bangladesh
- BJCSIRT, Benin
- BwCIRT, Botswana
- CI-CERT, Cote d’Ivoire
- DR-nCSIRT, Dominican Republic
- EG-CERT, Egypt
- BSSN, Indonesia
- MACRA, Malawi
- CERT-MU, Mauritius
- NITDA-CERRT, Nigeria
- Sri Lanka CERT|CC, Sri Lanka
- CERT.TG, Togo
- TTCSIRT, Trinidad and Tobago
- TunCERT, Tunisia
- CERTuy, Uruguay
- ZMCIERT, Zambia

- Vladim Aman, CICERT
- Palakiyem Assih, CERT.TG
- Vilius Benetis, NRD Cybersecurity, Lithuania
- Tracy Bills, CERT/CC
- Haythem El Mir, Keystone, Tunisia
- David Hunt, Prelude
- Jacomo Piccolini, Team Cymru
- Mahmoud Raouf, EG-CERT
- Don Stikvoort, Cyber4DEV
- Adli Wahid, APNIC

- Klée Aiken
- Abdul-Hakeem Ajijola
- Richard Harris
- Maarten van Horenbeeck
Questions and Discussion