NCSI
national cyber security index

45. Thailand 64.94

Population	**65.3** million	45th	**National Cyber Security Index**	‖‖‖‖‖‖‖‖‖‖‖‖‖ **65 %**
Area (km²)	**513.1** thousand	44th	**Global Cybersecurity Index**	‖‖‖‖‖‖‖‖‖‖‖‖‖‖ **87 %**
GDP per capita ($)	**18.7** thousand	78th	ICT Development Index	‖‖‖‖‖‖‖‖‖‖ **57 %**
		46th	Networked Readiness Index	‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖ **4 %**

NCSI DEVELOPMENT TIMELINE
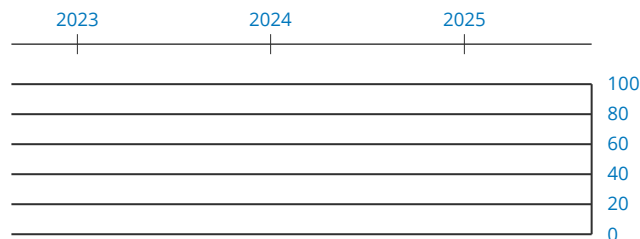
RANKING TIMELINE
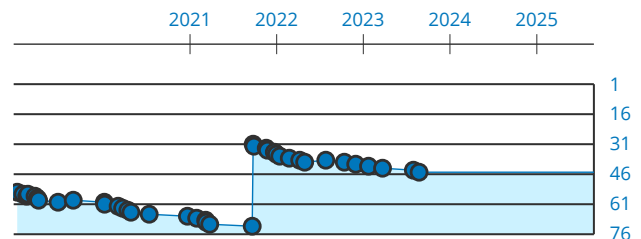
NCSI FULFILMENT PERCENTAGE

Policy · Threats · Education · Global · Digital · Essential · eID & TS · Personal · CIRC · Crisis · Police · Military
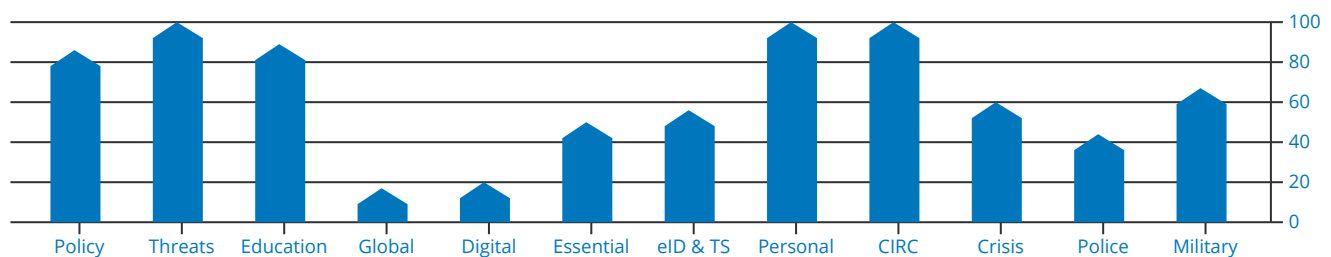
GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development — 6 → 7 (86%)
1.1. Cyber security policy unit — 3
1.2. Cyber security policy coordination format — 2
1.3. Cyber security strategy — 1
1.4. Cyber security strategy implementation plan — 0 / 1
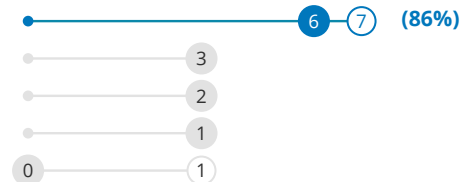
2. Cyber threat analysis and information — 5 (100%)
2.1. Cyber threats analysis unit — 3
2.2. Public cyber threat reports are published annually — 1
2.3. Cyber safety and security website — 1

### 3. Education and professional development — 8 → 9 (89%)
3.1. Cyber safety competencies in primary or secondary education — 0 / 1
3.2. Bachelor's level cyber security programme — 2
3.3. Master's level cyber security programme — 2
3.4. PhD level cyber security programme — 2
3.5. Cyber security professional association — 2
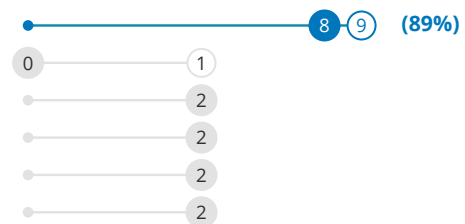
4. Contribution to global cyber security — 1 → 6 (17%)
4.1. Convention on Cybercrime — 0 / 1
4.2. Representation in international cooperation formats — 1
4.3. International cyber security organisation hosted by the country — 0 / 3
4.4. Cyber security capacity building for other countries — 0 / 1
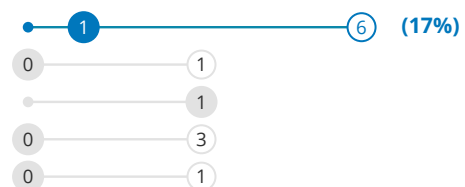
BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services — 1 / 5 (20%)

5.1. Cyber security responsibility for digital service providers — 0 / 1
5.2. Cyber security standard for the public sector — 1
5.3. Competent supervisory authority — 0 / 3

6. Protection of essential services — 3 / 6 (50%)

6.1. Operators of essential services are identified — 1
6.2. Cyber security requirements for operators of essential services — 1
6.3. Competent supervisory authority — 0 / 3
6.4. Regular monitoring of security measures — 1
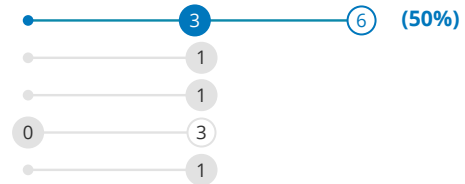
7. E-identification and trust services — 5 / 9 (56%)

7.1. Unique persistent identifier — 1
7.2. Requirements for cryptosystems — 0 / 1
7.3. Electronic identification — 0 / 1
7.4. Electronic signature — 1
7.5. Timestamping — 0 / 1
7.6. Electronic registered delivery service — 0 / 1
7.7. Competent supervisory authority — 3
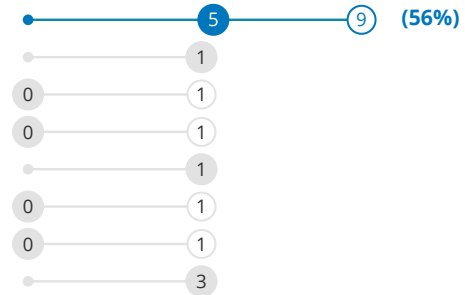
8. Protection of personal data — 4 (100%)

8.1. Personal data protection legislation — 1
8.2. Personal data protection authority — 3

INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response — 6 (100%)

9.1. Cyber incidents response unit — 3
9.2. Reporting responsibility — 1
9.3. Single point of contact for international coordination — 2

10. Cyber crisis management — 3 / 5 (60%)

10.1. Cyber crisis management plan — 0 / 1
10.2. National-level cyber crisis management exercise — 2
10.3. Participation in international cyber crisis exercises — 1
10.4. Operational support of volunteers in cyber crises — 0 / 1

11. Fight against cybercrime — 4 / 9 (44%)

11.1. Cybercrimes are criminalised — 1
11.2. Cybercrime unit — 3
11.3. Digital forensics unit — 0 / 3
11.4. 24/7 contact point for international cybercrime — 0 / 2

12. Military cyber operations — 4 / 6 (67%)

12.1. Cyber operations unit — 3
12.2. Cyber operations exercise — 0 / 2
12.3. Participation in international cyber exercises — 1