Safeguarding E-Government in a Cyber World

MR. MUHAMMAD UMAIR ALI & MS. HARISA SHAHID

Table of Contents

Definition

Electronic Governance is the application of Information and Communication Technologies (ICTs) for delivering government services through integration of various stand-alone systems between Government-to-Citizens (G2C), Government-to-Business (G2B), and Government-to-Government(G2G) services.

E-governance security can be defined as protecting citizen data, government operations, and critical infrastructure from a wide range of cyber threats,

Current E-Governance Landscape

- Website Development for Government Departments
- Online Forms and Services
- Digital Identity Document Management
- E-Voting
- Online Citizen Feedback and Complaint Filing System
- Digital Health Records
- Public Bidding Systems

Significance of Security in E- Governance

- Citizen Trust and Confidence:
- Protection of Sensitive Data
- National Security
- Data Privacy and Legal Compliance:

Cyberattacks

Malware Attacks

- Viruses
- Torjans
- Spyware

Data Breaches

- Abuse of authority
- Careless handling of data
- Mixing personal and private date

Phishing Attacks

- Email Phishing
- Speer Phishing
- Whaling

Cyber Espionage

- Social Engineering
- Catfishing

Country	National Cyber Security Index (NCSI)	Global Cybersecurity Index (GCI) 2020	Cybersecurity Exposure Index (CEI) 2020*	Cyber-Safety Score (Mean Average of NCSI and GCI)
1. Belgium	94.81	96.25	81.00	**90.69**
2. Finland	85.71	95.78	89.00	**90.16**
3. Spain	88.31	98.52	79.00	**88.61**
4. Denmark	84.42	92.60	88.30	**88.44**
5. Germany	90.91	97.41	75.90	**88.07**
6. Lithuania	93.51	97.93	70.30	**87.25**
7. France	84.42	97.60	77.20	**86.41**
8. Sweden	84.42	94.55	79.00	**85.99**
9. UK	77.92	99.54	79.30	**85.59**
10. Portugal	89.61	97.32	69.70	**85.54**

Lowest Risk Countries for Cyber Threats

HTTPS://SEON.IO/RESOURCES/GLOBAL-CYBERCRIME-REPORT/#:~:TEXT=HERE%20WE'VE%20LISTED%20THE,%2C%2018.60%2C%20AND%2019.72%20RESPECTIVELY

High-Risk Countries for Cyber Threats

Country	National Cyber Security Index (NCSI) (checked in 2023, Q1)	Global Cybersecurity Index (GCI) 2020	Cybersecurity Exposure Index (CEI) 2020*	Cyber-Safety Score (Mean Average of NCSI, GSI, and CEI)
1. Afghanistan	11.69	5.20	0.00	**5.63**
2. Myanmar	10.39	36.41	9.00	**18.60**
3. Namibia	15.58	11.47	32.10	**19.72**
4. Libya	10.39	28.78	20.70	**19.96**
5. Honduras	22.08	2.20	39.70	**21.33**
6. Cambodia	15.58	19.12	29.70	**21.47**
7. Mongolia	18.18	26.20	26.20	**23.53**
8. Ethiopia	32.47	27.74	13.40	**24.54**
9. Venezuela	28.57	27.06	19.30	**24.98**
10. Nicaragua	29.87	9.00	40.00	**26.29**

HTTPS://SEON.IO/RESOURCES/GLOBAL-CYBERCRIME-REPORT/#:~:TEXT=HERE%20WE'VE%20LISTED%20THE,%2C%2018.60%2C%20AND%2019.72%20RESPECTIVELY

Challenges and Best Practices for E-Government Security

Challenges in Securing E-Governance

1. Insider Threats
2. Vulnerability in Legacy Systems
3. Lack of cybersecurity awareness.
4. Budget Constraints
5. Technical Issues

Case Study: Cyberattack on Baltimore City

- Threat actors successfully deployed Robbin-Hood ransomware against the City of Baltimore in 2019, which ended up costing the city $18.2 million. The attack compromised the city's networks, took its email system offline, and adversely impacted its dispatch system.
- **Cyber-attack type:** Robbin-Hood ransomware
- **Location:** Baltimore
- **Cost:** $18.2 million
- **People affected:** Undisclosed
- The attackers demanded a payment of $76,000, which officials declined to pay. Ultimately, however, Baltimore experienced a loss that far exceeded the ransom request.

Best Practices for a Secure E-Government

- Use cloud-based technology
- Forge a dedicated National Critical Infrastructure Protection Pland and a Disaster Recovery Plan
- Switch to a .gov Domain
- Encrypt Sensitive Information
- Cyber Security Training for Employees
- Develop Cybersecurity Legislation and Compliance

Thank you