GS SCORE

Gist of Important REPORTS

FOR CIVIL SERVICE EXAM

GLOBAL CYBER-SECURITY INDEX 2017

GLOBAL CYBER-SECURITY INDEX 2017

The information and communication technologies (ICT) networks, devices and services are increasingly critical for day-to-day life. In 2016, almost half the world used the Internet (3.5 billion users) and according to one estimate, there will be over 12 billion machine-to-machine devices connected to the Internet by 2020. Yet, just as in the real world, the cyber world is exposed to a variety of security threats that can cause immense damage.

Statistics on threats to computer networks are sobering and reflect a shift from the relatively innocuous spam of yesteryear to threats that are more malicious. A security company tracking incidents in 2016 found that malicious emails became a weapon of choice for a wide range of cyberattacks during the year used by everyone from state sponsored cyber espionage groups to mass-mailing ransomware gangs. One-in-131 emails sent were malicious, the highest rate in five years.

Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. In some cases, organizations can be overwhelmed by the sheer volume of ransomware-laden emails they receive. Attackers are demanding more and more from victims with the average ransom demand in 2016 rising to USD 1 077, up from USD 294 a year earlier .

The scale of cybercrime makes it critical for governments to have a robust cybersecurity ecosystem in place to reduce threats and enhance confidence in using electronic communications and services. It is therefore clear that there is a direct cause-effect principle between the growth of ICTs and their illicit and malicious use.

To counter this effect, cybersecurity is becoming more and more relevant in the minds of countries' decision makers, and cybersecurity related doctrines have been established in almost all countries in the world. However, there is still an evident gap between countries in terms of awareness, understanding, knowledge and finally capacity to deploy the proper strategies, capabilities and programmes to ensure a safe and appropriate use of ICTs as enablers for economic development.

In this context, ITU, together with international partners from private-public and private sector as well as academia, has established the GCI with the key objective of building capacity at the national, regional and international level, through assessing the level of engagement of countries on cybersecurity, and, with the data gathered, producing a list of good practices that can be used by countries in need.

Index

GLOBAL CYBER-SECURITY INDEX 2017

About the Survey

The global community is increasingly embracing ICTs as key enabler for social and economic development. Governments across the world recognize that digital transformation has the power to further the prosperity and wellbeing of their citizens. In supporting this transformation, they also recognize that cybersecurity must be an integral and indivisible part of technological progress.

In 2016, nearly one percent of all emails sent were essentially malicious attacks, the highest rate in recent years. Ransomware attacks increasingly affected businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. Attackers are demanding more and more from victims, with the average ransom demand rising to over 1,000 USD in 2016, up from approximately 300 USD a year earlier. In May 2017, a massive cyberattack caused major disruptions to companies and hospitals in over 150 countries, prompting a call for greater cooperation around the world.

The Global Cybersecurity Index (GCI) is a survey that measures the commitment of Member States to cybersecurity in order to raise awareness.

The GCI revolves around the ITU Global Cybersecurity Agenda (GCA) and its five pillars (legal, technical, organizational, capacity building and cooperation).

The main objectives of the GCI are to measure:

- The type, level and evolution over time of cybersecurity commitment in countries and relative to other countries;
- The progress in cybersecurity commitment of all countries from a global perspective;
- The progress in cybersecurity commitment from a regional perspective;
- The cybersecurity commitment divide, i.e. the difference between countries in terms of their level of engagement in cybersecurity programmes and initiatives.

The objective of the GCI as an initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of commitment to cybersecurity worldwide.

Through the information collected, the GCI aims to illustrate the practices of other countries so that Member States can implement selected aspects suitable to their national environment, with the added benefits of helping harmonize practices and fostering, a global culture of cybersecurity.

The five pillars of the GCI are briefly explained below:

1. **Legal:** Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
2. **Technical:** Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.

Notes

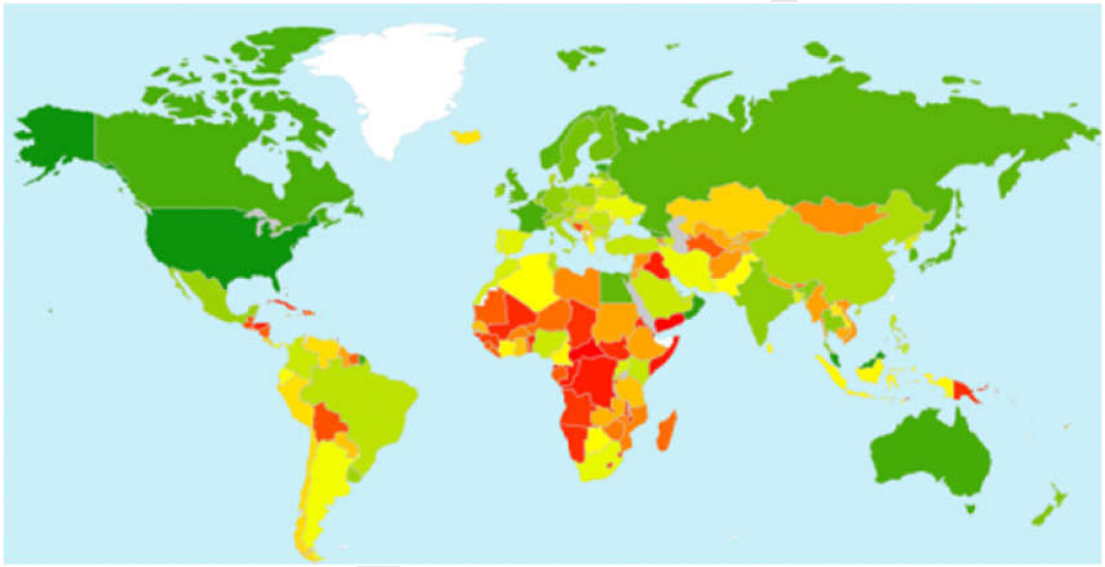
3. **Organizational:** Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

4. **Capacity Building:** Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.

5. **Cooperation:** Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.

Key findings

- **Heat Map of National Cybersecurity Commitments**
- Out of the 193 Member States, there is a huge range in cybersecurity commitments, as the heat map below illustrates. Level of commitment: from Green (highest) to Red (lowest)



Data is as follows:

Singapore, one of the world's smallest countries, has secured the first position in the UN (United Nations) list for global cybersecurity index. The report, Global Cybersecurity Index (GCI) 2017, showed that the Asian country has outshined some of the wealthiest and most powerful countries including United States, Australia, and France, according to Straits Times. The survey noted that Singapore has "a long history "of taking cyber security initiatives.

Among others, the top ten in the list are Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France and Canada. Russia ranked 11th.

The survey is divided into three stages, "initiating stage" - of countries started to make commitments in cybersecurity - this category has 96 countries that score less than the 50th percentile. "Maturing stage" - that have developed complex commitments, and engage in cybersecurity programmes and initiatives - it has 77 countries that score between the 50th and 89th percentile and the "leading stage" - 21 countries scoring in the 90th percentile with high commitment in all five pillars of the index.

India is ranked 23rd on the index with a score of 0.683 and has been listed in the "maturing" category, which refers to 77 countries that have developed complex commitments to cybersecurity and engage in cybersecurity programmes and initiatives.

Notes

Case studies

This is the important part of the report as the examples can be placed in the Mains answer or essays directly to increase the quality of content.

This chapter identifies noteworthy and thought-provoking practices in cybersecurity across the various GCI pillars. Examples are drawn from a number of countries and provide an insight on the cybersecurity commitment taken in their focus areas.

- **Cybercrime legislation**

COLOMBIA became one of the first countries in the world when, in 2009, it enacted a law specifically targeting cyberspace. Law 1273 (entitled "By means of which the Penal Code is amended, a new legal right is created - called 'protection of information and data'- and systems that use information and communication technologies are fully preserved, among other provisions") calls for a prison sentence or large fines for anyone convicted of information systems or telecommunication network crimes. The law covers areas such as illegally accessing personal information, intercepting data, destroying data or using malicious software.

GEORGIA established cybercrime legislation in line with the principles and rules of the Budapest Convention both in terms of substantive and procedural aspects. Illegal access to information systems, data and system interference, and misuse of devices are criminalized by the Georgia criminal code. The Personal Data Protection Act was enacted by Parliament in 2011 and is intended to ensure protection of human rights and freedoms, including the right to privacy, in the course of personal data processing.

- **Cyber security regulation**

SULTANATE OF OMAN established the eGovernance Framework, a set of standards / best practices and process management systems to enhance the delivery of government services in alignment with the mission of e.oman (Sultanate of Oman Digital Oman Strategy and eGovernment). The framework spells out the rules and procedures that ensure that government IT projects and systems are sustainable and in compliance with the Information Technology Authority (ITA) strategies and objectives. It provides assurance about the value of IT projects and framework for the management of IT-related risks. It helps in putting controls to minimize risks and better delivery of IT initiatives.

- **Cybersecurity training**

MAURITIUS makes available training for law enforcement and judiciary which has been conducted under the GLACY Project since 2013 and is still ongoing. CERT-MU also carried out cybersecurity trainings on digital forensic investigator professional and network forensic (packet analysis) for law enforcement officers. Training on information security standards and best practices is given to the technical officers of the IT Security Unit (ITSU) of the Ministry of Technology, Communication and Innovation.

The NEW ZEALAND (NZ) Police is introducing a 3-tiered training program for specialist cyber staff, investigators and then frontline staff. This is outlined in NZ Police's Prevention First National Cybercrime Strategy 2014-2017. NZ Police also provides training to the judiciary and prosecutors.

- **National CERT/CIRT/CSIRT**

EGYPT provides computer emergency response team (EG-CERT) support to several entities in the ICT sector, the financial sector as well as the government sector, in order to help them tackle cybersecurity related threats. EG-CERT is expanding and is currently upgrading its laboratories in the four key operational departments. Additional laboratories are being planned for mobile cybersecurity and industrial control systems cybersecurity.

Notes

- **Government CERT/CIRT/CSIRT**

LUXEMBOURG created a computer emergency response team (GOVCERT.LU) in 2011 to help protect government computer systems and data as well as specific infrastructures and is engaged at both national and international level under the name of NCERT. LU. GOVCERT.LU is also a critical player in the event of a large cyber-attack affecting country's ICT assets.

- **Cybersecurity standards implementation framework for organizations**

MALAYSIA created the Information Security Certification Body (ISCB), a department of Cybersecurity Malaysia, which manages information security certification10. The certification services are consistent with international standards and guidelines and include among others the Malaysian Common Criteria Evaluation and Certification (MyCC), which certifies security functions of ICT products based on the ISO/IEC 15408 international standard.

- **Child online protection**

SINGAPORE's Internet Content Providers (ICPs) and Internet Access Service Providers (IASPs) are licensable under the Broadcasting Act and they are required to comply with the Internet Code of Practice to protect children online. Since 2012, all service providers have been legally obligated to offer filtering services with Internet subscriptions and to make this known to consumers when they subscribe or renew. The Info-communications Media Development Authority also symbolically blocks 100 pornographic, extremist or hate websites.

- **Strategy**

UNITED KINGDOM issued in 2016 its second five years National Cyber Security Strategy. The strategy, issued by the Cabinet Office, aims to make the country one of the safest places in the world to carry out online business and doubles investment in cybersecurity compared to the first plan.

RUSSIAN FEDERATION officially adopted its National Security Strategy in 2000 and National Security Concept of the Russian Federation as well as Concept of the Foreign Policy of the Russian Federation in 2013. It established an Information Security Doctrine of the Russian Federation in 2000 and each government entity in the Russian Federation performs an annual audit of its own networks and systems in line with the doctrine and the areas identified in the various strategies adopted.

- **Responsible agency**

ICELAND created the Cyber Security Council, appointed by the Minister of the Interior that is responsible for overseeing the implementation of the National Cyber Security Strategy. In addition, a cyber security forum has been created as a collaborative venue for representatives of public bodies who sit on the Cyber Security Council and of private entities.

- **Cybersecurity research and development programmes**

GERMANY signed an agreement in 2009 on cooperation in IT security research between the Federal Ministry of Education and Research (BMBF) and the Federal Ministry of the Interior (BMI). The IT Security Research programme covers research and development in new information security technologies. The BMBF has been supporting three research centres since 2011 that bring together leading university and non-university establishments in cybersecurity.

KENYA EDUCATION NETWORK, (KENET), is the National Research and Education Network (NREN) of Kenya. KENET is the computer emergency response team (CERT) for the academic community and is licensed by the Communications Authority of Kenya (CA) as a not-for-profit operator serving the education

Notes

and research institutions. They most notably provide affordable, cost-effective and low-congestion Internet bandwidth services to member institution campuses in Kenya.

- **Public awareness campaigns**

LATVIA has published a series of articles on its national CERT portal about free-of charge security solutions including anti-viruses, firewalls, NoScript, etc. Twice a year, the national CERT organizes a campaign where people can bring their computers for a check-up to see if they are infected, and it also distributes commercial anti-virus installations during the campaigns that are made available free-of-charge for one year.

- **Cybersecurity professional training courses**

BULGARIA established the International Cyber Investigation Training Academy in 2009, which is a non-governmental organization. The academy aims to improve the qualification of specialists working in the field of cybersecurity. It has trained over 1 300 people from both the public and private sectors.

- **Public -private partnerships**

The UNITED KINGDOM is working with local company Netcraft on cyber security initiatives. This includes combatting phishing and malware hosted in the United Kingdom as well as phishing targeting the government. The partnership helped stop 34,550 potential attacks on government departments in the last six months of 2016, or 200 incidents a day.

- **Interagency partnerships**

The UNITED STATES OF AMERICA started its first cross-government security information sharing agreement in 2015. The Multilateral Information Sharing Agreement (MISA) binds government agencies from defence, health, justice, intelligence community and energy to work collaboratively to enhance cybersecurity information sharing, with an emphasis on information exchanges at machine speed.

SOUTH AFRICA established the national cybersecurity hub to serve as a central point for collaboration between industry, government and civil society on all cybersecurity incidents. The cybersecurity hub is mandated by the National Cybersecurity Policy Framework (NCPF) that was passed by Cabinet in 2012. The hub enhances interaction and consultations as well as promoting a coordinated approach regarding engagements with the private sector and civil society.

Conclusion

Cybersecurity is an increasingly important part of our life today, and the degree of interconnectivity of networks implies that anything and everything can be exposed, and everything from national critical infrastructure to our basic human rights can be compromised. Governments are therefore urged to consider policies that support continued growth in technology sophistication, access and security, and as a crucial first step, to adopt a national cybersecurity strategy.

For the Global Cybersecurity Index to have an impact on raising awareness on this crucial emerging concern over time, continuity of the GCI effort is essential. ITU therefore welcomes all Member States and industry stakeholders to actively participate in future efforts to enhance the current reference model. As well, the success of future iterations of the GCI largely depends on the engagement of Member States and the quality of their responses to the questionnaire, and ITU calls on all Member States to take part in the next GCI survey. ITU would like to thank all Member States for their valuable support for the conduct of the GCI survey and the publication of this report as well as future ones.

Notes