FORUM: United Nations Commission on Science and Technology for Development

QUESTION OF: Measures to Robust Data Privacy and Protect Cybersecurity in the Digital Age.

MAIN SUBMITTER: Chile

CO-SUBMITTERS: Cambodia, Russia, South Sudan, Belgium, India, Senegal, Republic of Korea, France

UNCSTD,

*Realizing* that the economic cost of information and technology asset security breaches in 2020 was a staggering USD 4-6 trillion, equivalent to about 4-6% of global GDP,

*Emphasizing* that an average of 8,000,000 cybercrimes per year are happening in the world,

*Recalling* the importance of digital is becoming more critical in our society, where about 5.44 billion people were using the Internet as of July 2024,

*Noting* that Nearly 1 billion emails are exposed to cybercrime in a single year,

*Fully believing* that personal data is a basic right of individuals, and its protection is essential to the freedom and privacy in the digital age,

*Aware of* the rising risks and occurrences of identity theft, fraud and other cybercrimes through data leaks and exposing personal information due to the digital age,

*Recognizing* that unexpected data leaks can lead to massive data attacks, greater worsening cybersecurity concerns,

*Noting* that the European Union General Data Protection Regulation (GDPR) is the most prominent data privacy and security laws in the world,

1. Calls for the establishment of an international department dedicated to addressing cyberattack incidents, with the primary goals of responding to cybersecurity crises, improving cybersecurity defenses, and identifying the sources of attacks and cybercriminals in such ways but not limited to:
   1. Advocates for international department to develop a framework to address the global impact of cybersecurity risks with international significance, including:
      1. establishing joint methodologies for evaluating cybersecurity vulnerabilities across borders,
      2. Promote harmonization of cybersecurity regulations to ensure consistent protective measures around the world,
   2. Record cybercrimes and breaches reported by member states, organizations, and private entities and provide it to the public through open- source platforms, recording information including:
      1. Scale of the attack,
      2. Impact of the attack,
      3. Type of the attack,
   3. Encourages member states to cooperate in the exchange of information on cyberattacks in ways such as but not limited to:
      1. improve defenses against attack by identifying patterns and weaknesses in cyberattack strategies,
      2. aid the attribution of cyberattacks, increasing accountability,
2. Urges member states to implement and enforce robust and proactive cybersecurity regulations by taking decisive actions aimed at protecting digital infrastructure, safeguarding sensitive data, and minimizing the risk of cyber threats in ways such as but not limited to:
   1. Establishing regular software updates to ensure that all systems and applications are protected from vulnerabilities in such ways but not limited to:
      1. mandating automatic updates where feasible,
      2. conducting audits to verify compliance,
      3. proving resources for software management,
   2. Encourages nations to establish strong password policies that follows:
      1. complexity requirements to enhance password strength,
      2. regular updates and rotation of passwords,
      3. encouraging the use of password managers for better security,
   3. Implementing multi-factor authentication (MFA) across all critical systems to:
      1. providing an additional layer of security for user accounts,
      2. reducing the risk of unauthorized access,
      3. ensuring accessibility measures are in place for users,
3. Raising awareness to a bigger audience to raise the understanding and maximize the potential of setting individuals’ personal privacy mindsets, empowering them to take proactive steps in protecting their personal information and recognizing the importance of safeguarding their digital identities in ways such as but not limited to:
   1. Making videos and visual campaigns for establishing a basic understanding of digital privacy and for promoting clear and transparent communication and presenting in public events and platforms, such as but not limited to:
      1. Government websites,
      2. Social media platforms,
      3. Speeches reflecting the government’s perspective,
   2. Visual communications should include content to expand on the public's idea of the digital age in areas such as but not limited to:
      1. reminding the importance of personal privacy and the advantages of the developments in the digital age,
      2. introducing real-life examples of privacy issues during the digital age,
      3. showing consequences to individuals after facing privacy issues during the digital age,
   3. Research the impact of digital surveillance and privacy breaches on individuals and societies and publish findings to inform policy development:
      1. undertake comprehensive research projects that assess the social, economic, and psychological consequences of digital privacy infringements,
      2. share research findings with governments, international organizations, and the private sector to inform policy and practice,
4. Encourages the establishment of national data privacy laws that strictly govern the collection, storage, and use of personal information, ensuring that individuals' privacy rights are respected and always protected, such as but not limited to:
   1. Create laws that ensure personal data is used and collected safely so that individuals will not be victims of identity theft and data breaches in ways such as but not limited to:
      1. personal data will be collected based on clear and explicit consent from individuals,
      2. individuals will be fully informed about how their personal data will be stored, collected, used and shared,
   2. Ensure that laws of the collection and sharing of personal information and data include provisions and robust rules that ensure things such as:
      1. ensuring that individuals have the right to access, correct, or delete their personal data at any time,
      2. transparency of third-party data sharing and the purpose of collecting and sharing data,
   3. Encourages government to establish data protection authorities in such was but not limited to:
      1. oversee compliance with data privacy laws and regulations,
      2. execute penalties for violating the law, ensuring strong restrictions on non- compliance,
   4. Establish strict punishments for cybercriminals who commit cybercrimes and malicious activities on digital platforms or networks in such ways but not limited to:
      1. Monetary fines,
      2. Imprisonment for severe offences,
5. Urges all countries to establish a fund-raising system to provide financial support for victims of cybercrime and security issues and to ensure that affected individuals and organizations receive the resources needed to recover cybersecurity defenses such as but not limited to:
   1. Raising funds through methods such as but not limited to:
      1. Donations from high-income countries (HIC) countries,
      2. Donations from non-government organizations (NGOs) and charity funds organizations,
      3. Donations from individuals willing to donate through funds’ website,
      4. Donations from cooperating enterprise or international partner companies,
   2. The funds will be supervised in ways such as but not limited to:
      1. The fund's database will be required to publish and share publicly across relevant countries an annual report that includes but is not limited to the money sources, money flow, and money usage,
      2. Establish a window on the funds' website to accept the report from the public,
      3. All the funds will be checked between countries for supervision,
6. Recommends all nations strengthen and expand cybersecurity education and training programs, with the goal of enhancing the technical skills of citizens, enabling them to better understand, prevent, and respond to the growing threat of cybercrime through such ways but not limited to:
   1. Encouraging the establishment of professional programs for government officials and business leaders, focusing on:
      1. Practices in securing digital infrastructure, understanding current threats, and responding to occurrences,
      2. Implementing robust cybersecurity structure within organizations,
      3. Establishing monthly or annual meeting to make sure that government officials and business leaders to fully understand the problems about cybersecurity risks and the urgent methods to solve,
   2. Encouraging schools to offer education programs to students in such ways but not limited to:
      1. Including cybersecurity as part of the school standard curriculum,
      2. Providing selective courses about cybersecurity to higher education students,
   3. Recommending the creation of public education programs on cybersecurity, such as but not limited to:
      1. Online courses,
      2. Workshops,
      3. Certification programs,
7. Calls for the development of mandatory cybersecurity testing including National Cybersecurity Readiness Index (NCRI), to evaluate and enhance the preparedness of governments, industries, and organizations to resist cyber threats through actions such as but not limited to:
   1. Establishing the NCRL to create a standardized cybersecurity criteria to assess the preparedness of national infrastructures, industries, and organization to address potential cyber threats and require governments to report the outcomes of the test to their citizens to detail improvements and plans to address identified cybersecurity weaknesses,
   2. Mandating regular governments and important infrastructure sectors to conduct Cybersecurity Resilience Tests (CRT) to stimulate real-world cyberattacks, to evaluate their ability to detect and respond to incidents, using tests with various attack vectors such as:
      1. Ransomware,
      2. DDoS attacks,
      3. Supply chain vulnerabilities.