CYBER MANIPULATION

Guarding against digital threats, data breach

MOHD NOOR OMAR

BEYOND land, sea, air, and space, there is a fifth domain — cyberspace. Data is the new soil and water for life, and data is also a new threat as the digital economy is not an option, but a must. In today's interconnected society, no one is safe from cyber vulnerabilities.

The Malaysia Digital Economy Blueprint maps out a direction and plan for a better future. Post-pandemic norms are witnessing new business models on digital platforms.

The online marketplace and digital commerce segment became the most favourable transaction preference and the total transaction is projected to reach US$10.919 million next year, with an annual growth rate of 15.97 per cent.

Cyberspace is a hidden battlefield, where nations wage secret wars. Trust, justice, freedom, equality, rights, privacy, and even religion is at stake. Cybercrime, hacking, data breach, and manipulation definitely are unavoidable trade-offs for digital transformation.

Data breach is an act of releasing a secure or confidential information to an untrusted party or environment. Cyber-espionage is the use of computers to access confidential information, also known as cyberspying. People, governments, and corporations are vulnerable to those threats and data breaches.

We all know those terms, but how prepared are we in overcoming them? We might wonder how the system will suggest a piece of information from our search history whenever we revisit the same platform or another.

That is the simplest example is how our data and activities are being manipulated by the algorithm and programming in cyberspace, prompting your preferences or even generating your complete profile based on what you have searched, watched or visited on the Internet.

The data is important for marketing purposes and is valuable to third parties in digital marketing. There are dangers in being so connected. High-profile international hackers have shown that they have the potential to cause physical damage and loss of life as well.

The nature of the threat is evolving all the time and could cause racial tension, religious distress, international conflict, and political unrest. No agency or even the government as a whole can manage cybersecurity by itself. The more technology we use, the more vulnerable we become because the technology itself is the medium.

We should not assume that we are immune. The attacker is always eyeing how to creep into government servers, banks, organisation databases or even personal information, such as passwords. There are more than 4.66 billion Internet users who send and receive a huge amount of data every day.

Their data packets are ultimately directed around the world by 80,000 autonomous routers. The routers run the Internet's traffic control system through the Border Gateway Protocol (BGP), initially designed based on trust, where every player is expected to perform their best norm as they can. But, the BGP router can be tricked and could be used to redirect data packets off course, which can be monitored and intercepted by cyberspies.

The online marketplace and digital commerce segment has become the most favourable transaction preference. FILE PIC

Technically, there is no solution to prevent hijacking of the data superhighway. Apart from improving awareness through digital literacy, the digital defence for the security pillar should be established.

The relevant consultative body should deal with potential challenges and threats, as well as how to respond in the digital risk and crisis. A cyber threat analysis must be made known to industries, clusters, or potential targeted groups. An application or software should be screened for potential violation of rights and privacy before it is allowed.

We really need to have a capable device and mechanism to access it. Technological incapability is a critical weakness. Cyberspies can even hack the infrastructure that supports the Internet. We should also revisit our laws and enforcement to strengthen our legal provisions to protect the data and information from breach.

Recently, a United States District judge had approved a privacy suit under Illinois' Biometric Information Privacy Act, awarding US$650 million to Facebook users who alleged the company created and stored scans of their faces without permission. Facebook is the biggest social media platform used by Malaysians (89.54 per cent), compared with the others, YouTube (3.03 per cent), Pinterest (2.98 per cent), Twitter (2.73 per cent), Instagram (1.24 per cent) and Reddit (0.24 per cent), which could also be targeted for the same purpose.

The digital economy is not only about opportunities, but also potential vulnerabilities. Planning, preparation, expertise and infrastructure should be developed from time to time along technological advancements to align with unpredicted future threats.

The writer is fellow, Centre for the Study of Shariah, Law, and Politics, Institute of Islamic Understanding Malaysia (Ikim)