ESTABLISHING AN APPROPRIATE FRAMEWORK FOR MEANINGFUL CYBER-THREAT INFORMATION SHARING

Cybersecurity incidents or breaches can have a major impact on governments and private entities, as well as individuals. Some high-profile breaches have encouraged governments around the world to consider how to best prevent, detect and react to these incidents.

The exchange and sharing of the appropriate information at the right time — and the coordinated effort among relevant actors that it enables — is considered the best way to reduce and mitigate risks and respond to cyber incidents.

Accordingly, the key question is how to best achieve meaningful and effective information sharing among relevant stakeholders. While some countries have considered mandatory incident notification systems, these alone would not suffice to address the issue of collective awareness and preparedness. When it comes to that, voluntary information exchanges based on trust have proved to be the most efficient way to achieve successful information sharing.

Such meaningful information sharing is not an easy undertaking. It can only be achieved if the necessary environment facilitating such exchanges is in place. Some of the fundamentals of such an environment are the following:

- **Create an environment of trust:** Cyber-threat information sharing, as well as incident reporting, require safeguards and incentives for their effective functioning. These elements help ensure the trust necessary for the operation of such a system. They include guarantees that the sharing of information will not subject the organization providing these to undue liabilities, public humiliation, litigation or sanctions.

- **Ensure a high level of confidentiality:** Given the sensitive nature of the information shared about an incident or cyber threat affecting any critical infrastructure, it is crucial to ensure that confidentiality and security of the communications between the infrastructure operator and any supervisory authorities are respected and maintained, subject to transparent reporting by the authority, as appropriate.

  Nevertheless, in some cases, informing the public of an incident may be necessary. In these instances, all care should be taken to ensure an in-depth dialogue between the entities suffering a breach and the authorities before any disclosure in order to avoid increasing the attack surface, multiplying the impact of the incident, creating panic, or leading to undue public shaming.

- **Ensure reciprocity:** While the private sector owns and operates much of the countries' critical infrastructure, information sharing should not be seen as a one-way provision of relevant data from private to public entities. It should be regarded as a real and mutual exchange of information, based on trust and mutual benefits.

- **Make requirements clear and consistent across jurisdictions:** As mandatory notification requirements cover an ever-increasing number of areas and geographies, the likelihood of facing conflicting legal obligations increases. As various organizations operate in multiple sectors across different countries and regions, the questions of what to report when and to whom already pose important compliance challenges. Therefore, to the extent a mandatory notification system should be introduced, it is imperative to strive for as much consistency as possible not only among the different notification obligations, but also among the various national and regional requirements.