Strengthening the Cyber Security Ecosystem of Bangladesh

Farhad Hussain

Technical Specialist, Leveraging ICT for Growth, Employment and Governance Project, Bangladesh Computer Council

The cyber security ecosystem is global, evolving and includes government and private sector information infrastructure; the interacting persons, processes, data, information and communications technologies; and the environment and conditions that influence cyber security. As part of its ambition to strengthen and consolidate it's positioning in the ICT field, also attested by its "Digital Bangladesh" initiative, Bangladesh needs to position cyber security as a matter of high priority, particularly to remain an attractive and competitive location for all companies already doing business or aiming at setting up their operations in Bangladesh.

At present, cyber defenses in organizations across Bangladesh largely rely on ad hoc, manual processes. Unfortunately, cyber criminals often plan attacks in a systematic fashion, starting with reconnaissance activities and escalating to more sophisticated and devastating levels of system entry. This leaves us struggling to keep up. As Bangladesh strives to ensure that state-of-the-art technology is enabled, better cross fertilization among the cyber security organizations is necessary, which have to operate in an ever-changing ecosystem. There should be a strong incentive, willingness and need for governmental bodies and companies to come together and jointly agree on an action plan. The first task at hand should be better connecting, across the board between the key contact points and mission statements of relative government agencies. Moreover, creating and implementing competitive and state-of-the-art cyber security legislation and including cyber security in the national ICT strategy at the same time, would greatly help Bangladesh become a benchmark in the cyber security landscape.

An effective cyber security ecosystem requires not only the continual development of efficient cyber defense processes and technologies, but also a close collaboration between the public and private sectors. The effectiveness and resilience of this ecosystem, however, can be hampered by the cyber threats in today's connected digital world. As cyber attacks become increasingly sophisticated, complex and difficult to detect, advanced solutions that enable seamless security processes are essential. It is also no longer feasible for a single entity to rely on its own capabilities to defend against such cyber attacks. There is a crucial need for the various entities in the cyber environment to work together to tackle the challenge.

Accordingly, the Government, the academia and industry partners need to develop a close partnership that will enable such initiatives and measures as the sharing information, the development of innovative cyber solutions, the training of the next generation of cyber security professionals and the establishment of local operational and research facilities. These and other collaborative efforts of all stakeholders will aid in the shaping of a cyber security ecosystem that is both robust and vibrant. The cyber security ecosystem can broadly be divided into two categories, with some players (e.g. governments) having roles in both categories. The following figure depicts an indicative model of cyber security ecosystem.

Macro-level players: Consists of those stakeholders who are in a position to exert influence on the way the cyber security field looks and operates at the micro-level. Key examples include governments, regulators, policymakers and standards setting organizations and bodies (such as the International Organization for Standardization, Internet Engineering Task Force and National Institute for Standards and Technology).

Micro-level players: Consists of those stakeholders who, both collectively and individually, undertake actions on a day-to-day basis that affect the community's overall cyber security posture. Examples include end users/consumers, governments, online businesses, corporations, SMEs, financial institutions and security consultants.

The macro level has, in the past, been somewhat muted with its involvement in influencing developments in cyber security. Governments and regulators, for example, often operated at the fringes of cyber security and primarily left things to the micro-level. While collaboration occurred in some instances (for example, in response to cyber security incidents with national security implications), that was by no means expected.

Nevertheless, we are now regularly seeing more formalized models being introduced to either strongly encourage or require collaboration on cyber security issues between multiple parties in the ecosystem. Recent prominent examples include proposed draft legislation in Australia that would, if implemented, require nominated telecommunications service providers and network operators to notify government security agencies of network changes that could affect the ability of those networks to be protected, proposals for introducing legislative frameworks to encourage cyber security information sharing between the private sector and government in the United States, and the introduction of a formal requirement in the European Union for companies in certain sectors to report major security incidents to national authorities.

The universe of cyber space is made of diverse entities that interact in ever-changing ways, much like in the natural world. From people with laptops, smart phones, and tablets, to companies and government agencies with computers and servers – not to mention all the data those devices contain - this "cyber space" creates a target-rich environment. Malicious individuals or groups exploit vulnerabilities to steal identities, resources, and competitive secrets. And with cyber attacks on the rise, economic security and the continuity of businesses and government services are at risk.

To address this risk, we must develop "the cyber security ecosystem of the future," a place where private industry, academia, and the government can work together quickly to predict when cyber attacks might take place, limit their spread, and minimize their consequences. The key elements of effective cyber security are threat intelligence, automation, interoperability, and authentication. With these building blocks in place, companies and government agencies would have much more effective tools to identify and respond to data or network breaches. There are several key attributes of a healthy cyber security ecosystem, which are the following:

Information is connected across space and time. Information created in one part of the ecosystem conveys rapidly to others, and can be configured to protect sensitive data.

Rapid and universal learning. Machines learn from each other and people learn from machines.

Greater attribution. Machines and people work together to improve data attribution.

Emerging analytics. Data from multiple, discrete sources are fused and aggregated to create new intelligence.

Greater network reach. Security content is separated from delivery mechanisms and managed as an ecosystem asset.

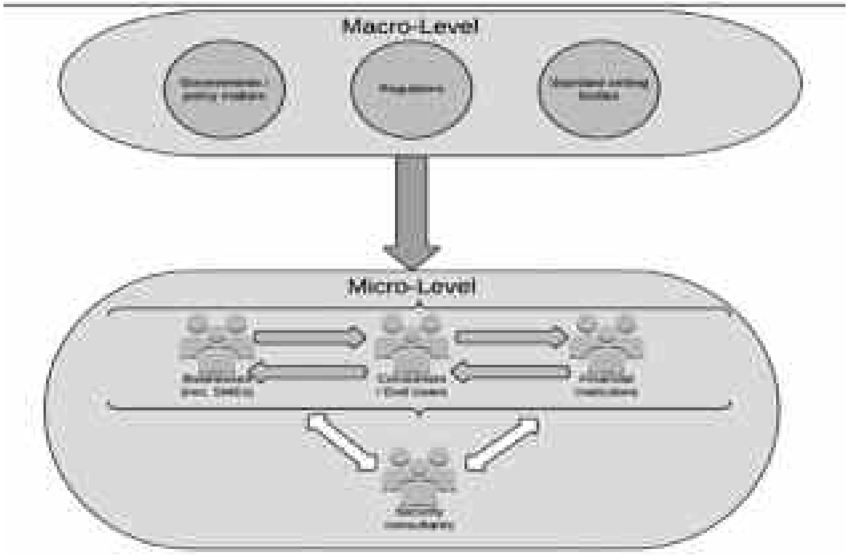
New defensive tactics. Attacks only work once, if at all.

Lifecycle feedback. Rich feedback loops from the front end of system and technology life cycles reduce costs, shorten adoption cycles, and improve ecosystem health.

Traditional approaches for cyber security that focus inward on understanding and addressing vulnerabilities, weaknesses, and configurations are necessary but insufficient in today's dynamic cyber landscape. Effective defense against current and future threats also requires the addition of an outward focus on understanding the adversary's behavior, capability, and intent. Only through a balanced understanding of both the adversary and ourselves can we understand enough about the true nature of the threats we face to make intelligent defensive decisions. The development of this understanding is known as cyber threat intelligence (CTI). Cyber threat intelligence itself poses a challenge in that no single organization can have enough information to create and maintain accurate situational awareness of the threat landscape. This limitation is overcome by sharing of relevant cyber threat information among trusted partners and communities. Through information sharing, each sharing partner can achieve a more complete understanding of the threats they face and how to defeat them.

The proliferation of hacking activities, coupled with the growing cyber threats associated with mobile devices, cloud computing, financial technology and targeted attacks on critical infrastructures, have posed ever-increasing challenges on cyber security. To maintain a secure, stable and reliable e-government and e-business environment it is indispensable to strengthen the Cyber Security Ecosystem of Bangladesh ◙

The Cyber Security Ecosystem


Macro-Level
Micro-Level