The world is hardly wired for cyber resilience

Defending civilian targets and infrastructure against rising cyberattacks will stretch the capability of governments

M.K. NARAYANAN

A string of high-profile cyberattacks in recent months has exposed vulnerabilities in the critical infrastructure of even advanced nations. This has reinforced the need for improved defences against actual, and potential, cyberattacks by all countries across continents.

America under attack

Several high-profile cyberattacks were reported from the United States during the past several months. Towards the end of 2020, for instance, a major cyberattack headlined 'SolarWinds' – and believed to have been sponsored from Russia – had rocked the U.S. It involved data breaches across several wings of the U.S. government, including defence, energy and state. Before the U.S. could even recover from this breach, thousands of U.S. organisations were hacked in early 2021 in an unusually aggressive cyberattack, by a Chinese group Hafnium, which had exploited serious flaws in Microsoft's software, thus gaining remote control over affected systems.

In quick succession, thereafter, the U.S. has witnessed three more major attacks: an audacious ransomware attack by Russia/East Europe-based cybercriminals, styled DarkSide, on Colonial Pipeline (which is the main supplier of oil to the U.S. East Coast), compelling the company to temporarily shut down operations. The siege was lifted after Colonial Pipeline paid out several million dollars as ransom to unlock its computers and release its files. There are reports of the ransom being received in bitcoins which was later seized by the U.S government. Another Russia-backed group, Nobellium, next launched a phishing attack on 3,000 e-mail accounts, targeting USAID and several other organisations. Early this month, JBS SA, the U.S. subsidiary of a Brazilian meat processing company, was the target of a ransomware attack; the company also paid a ransom in millions.

Now, civilian targets

These attacks were all primarily on civilian targets, though each one was of critical importance. Obviously cyber, which is often referred to as the fifth domain/dimension of warfare, is now largely being employed against civilian targets, bringing the war into our homes. Most nations have been concentrating till date mainly on erecting cyber defences to protect military and strategic targets, but this will now need to change. The obsession of military cyber planners has been to erect defences against software vulnerabilities referred to as 'Zero-day', that had the capability to cripple a system and could lie undetected for a long time. (The most celebrated Zero-day software of this kind to date is Stuxnet, which almost crippled Iran's uranium enrichment programme some years back). Today, other Zero-day software, no doubt exist, though little is known about them. What is, however, evident is that a whole new market currently exists for Zero day software outside the military domain, and the world must prepare for this eventuality.

Defending civilian targets, and more so critical infrastructure, against cyberattacks such as ransomware and phishing, including spear phishing, apart from unknown Zero day software, is almost certain to stretch the capability and resources of governments across the globe, somewhat in the manner that nations have been forced to find the resources and the methods to deal with the COVID-19 pandemic. One related problem is that the distinction between military and civilian targets is increasingly getting erased and the consequences of this could be indeterminate. For instance, the 2012 cyberattack on Aramco, employing the Shamoon virus, which wiped out the memories of 30,000 computers of the Saudi Aramco Oil Corporation, has ever since been one reason for the very frosty relations between different countries in West Asia and the Gulf region.

GETTY IMAGES/ISTOCKPHOTO

Cyber warfare is replete with several damaging methodologies. In the civilian domain, two key manifestations of the 'cat and mouse game' of cyber warfare today, are ransomware and phishing, including spear phishing. Ransomware attacks have skyrocketed, with demands and payments going into multi-millions of dollars. India figures prominently in this list, being one of the most affected. Also experts believe that of late, the recovery cost from the impact of a ransomware attack – in India, for example, has tripled – and mid-sized companies, in particular, today face a catastrophic situation, if attacked, and may even have to cease operations. Thus, the need to be aware of the nature of the cyber threat to their businesses and take adequate precautionary measures, has become extremely vital. Banking and financial services were most prone to ransomware attacks till date, but oil, electricity grids, and lately, health care, have begun to figure prominently.

Zeroing in on health care

What is specially worrisome at this time, when a pandemic is raging, is the number of cyberattacks on health-care systems. With data becoming a vital element in today's world, personal information has become a vital commodity. One of the more vulnerable areas where data tends to be linked to a specific individual is in health care. Compromised 'health information' is proving to be a vital commodity for use by cybercriminals. All indications are that cybercriminals are increasingly targeting a nation's health-care system and trying to gain access to patients' data. The available data aggravates the risk not only to the individual but also to entire communities.

It would be a mistake to believe that we can hope for a respite from cyberattacks such as ransomware and phishing. Cybercriminals are becoming more sophisticated, and are now engaged in stealing sensitive data in targeted computers before launching a ransomware attack. This is resulting in a kind of 'double jeopardy' for the targeted victim. Also, today's cybercriminals, specially those specialising in ransomware and similar attacks, are different from the ordinary run-of-the-mill criminals. Many are known to practise 'reverse engineering' and employ 'penetration testers' to probe high secure networks.

The bad news is that the cyber landscape is poised to undergo more fundamental changes. Motivation for cyberattacks vary: for (some) nation states, the motivation is geopolitical transformation; for cybercriminals, it is increased profits; for terror groups, the motivation remains much the same, but the risk factor may be lower. However, it is 'insider threats' – due to discontent with the management or for personal reasons – that could well become an omnipotent reality.

Need for data protection

Cybersecurity essentially hinges on data protection. As data becomes the world's most precious commodity, attacks on data and data systems are bound to intensify. Reportedly, we create more than three quintillion bytes of data everyday (some put it at over 2.5 quintillion) – with several billion devices interconnected to billions of end point devices exchanging petabytes of sensitive data, on the network. This is only bound to grow. Ensuring data protection could, hence, prove to be a rather thankless task, complicating the lives of Information and other security professionals.

The data life cycle can broadly be classified into data at rest (when it is being created and stored), data in motion (when it is being transmitted across insecure and uncontrolled networks), and data in use (when it is being consumed). Constant exposure lends itself to ever increasing data thefts and abuse. With mobile and cloud computing expanding rapidly, and also given the nature of the on-going pandemic, cybersecurity professionals are now engaged in building a 'Zero Trust Based Environment', *viz.*, zero trust on end point devices, zero trust on identity, and zero trust on the network to protect all sensitive data. What is of interest is that there do exist quite a few niche companies today, which have developed (or are developing) newer technologies to create a Zero Trust Based environment employing: software defined solutions for agile perimeter security, secure gateways, cloud access security, privileged access management, threat intelligence platforms, static and dynamic data masking, etc. The moot point is whether not only those in authority but even more so those in the world of business, (specially oil and finance, and specifically health care) are aware of this – and, more important, are ready to utilise these technologies – to ward-off a cyberattack and safeguard their data.

Preparation is needed

Building deep technology in cyber is essential. New technologies such as artificial intelligence, Machine learning and quantum computing, also present new opportunities. Nations that are adequately prepared – conceptually and technologically – and have made rapid progress in artificial intelligence and quantum computing and the like will have a clear advantage over states that lag behind in these fields. Pressure also needs to be put on officials in the public domain, as also company boards, to carry out regular vulnerability assessments and create necessary awareness of the growing cyber threat. In the end, it might be appropriate to quote IBM Chairman, Arvind Krishna, that cybersecurity will be "the pressing issue of this decade" and that "value lies in the data and people are going to come after that data".

M.K. Narayanan, currently Executive Chairman of CyQureX Pvt. Ltd., a U.K.-U.S.A. cybersecurity joint venture, is a former National Security Adviser and a former Governor of West Bengal