Fighting the Ransomware

Why in news?

\n\n

Ransomware has been contained globally, but the threat is not completely eliminated.

\n\n

What is the issue?

\n\n

\n
- One group of hackers picked up cyber tools stolen by another from America's National Security Agency, and then effectively "weaponized" them to hold hostage millions of computers across the world.
\n
- Users, mostly using older version of the Microsoft Windows software, were locked out of their computer and told to pay a ransom in bitcoins if they wanted to get back in.
\n
- Though the attack was contained soon enough, the ransomware still managed to infect many European Public systems, Universities in China and a multinational courier delivery company in the US.
\n
- India was reportedly one of the worst-affected countries although, notably, no major mass disruptions were reported.
\n
- As for the hackers, they made just about a paltry $100,000 in bitcoins which they are unlikely to be able to access anytime soon.
\n

\n\n

How such kind of attacks can be prevented?

\n\n

\n
- A good starting point is the three-layered Israeli strategy that goes beyond

security to build a cyber system that is robust, resilient and has strong defence capabilities.
\n
- Think of the country’s IT infrastructure as a human body.
\n

\n\n

\n
- The first level, the body needs a robust immune system to protect it from everyday attacks without disrupting the flow of work.
\n
- The second level—that of building resilience, Think of the Indian Computer Emergency Response Team as the cyber equivalent of the Centres for Disease Control and Prevention in the US.
\n
- The third level is that of national defence, wherein there is a direct threat to the state and its citizens. The government takes the lead role here but, importantly, its success depends on the robustness and resilience of the system as a whole.
\n

\n\n

What is the status of the threat?

\n\n

\n
- The fact that this attack could have been much worse had it, for example, not been designed to extort money but to actually take down critical infrastructure systems, high-value military targets or even nuclear installations.
\n
- Yet, as this latest attack testifies, the world is still playing catch-up and several vulnerabilities remain.
\n
- The vulnerabilities will continue to grow as our daily lives are further integrated into the cyber arena.
\n
- The situation is arguably worse in developed nations which are far more dependent on the Internet—for example, last year hackers broke into a US water supply company and manipulated its water treatment systems.
\n
- But developing countries, including India, can hardly afford to be complacent. After all, if cyberattacks in previous years could lead to huge monetary losses, today they can cost lives.

\n

\n\n

What is the way forward?

\n\n

\n
- Traditional security concepts and frameworks have struggled to adapt in the cyber arena.
\n
- The lack of cybersecurity is a real concern, posing an imminent threat to the life and well-being of citizens, few states take direct responsibility for the cybersecurity of civilian assets.
\n
- This includes not just critical infrastructure networks such as power lines and stock markets but also individuals and business organizations.
\n
- In the cyber realm, it is equally difficult to trace and track the enemy; and even when one is neutralized, several others appear in no time.
\n
- Fighting this hydra-headed monster is a challenge, to say the least, but it is one that must be tackled head on.
\n
- This has to be a collective effort involving all stakeholder industry, academia, foreign partners and private individuals.
\n

\n\n

\n\n

Source: Live Mint

\n