New tech that can fight cybercrime in the year 2020

Technological advances are taking place more rapidly than they are being adopted on ground. More devices and individuals are getting connected to cyberspace and are exposed to online risks. Intel Corp. predicts the number of internet-connected devices to go from the current 15 billion to around 200 billion in 2020—which is also the number of potential devices that might be prone to being hacked. In the present scenario, businesses face difficulty in securing their assets from potential threats; imagine the risk of cybercrime with 200 billion devices coming online.

While there is no denying the future threats of cybercrime, we simply cannot undermine the importance and risks associated with upcoming technology. Connecting cars, planes, pacemakers and even power grids to computer systems has given us more access to the immense efficiency and automation than was unimaginable some decades ago. So will be the growth in security threats that come attached to the connected cyberspace.

Here are some of the areas that future cyber criminals would focus on.

Data protection and privacy: The parameter of data protection already serves as a great challenge with respect to online services. The future of data aggregation, globalized sensor proliferation, and personalization would require the augmented services to adopt common legal frameworks to ensure security and privacy. Countries might exercise sovereignty rights for setting their specific rules with respect to when data should be stored and processed by different authorities for reliable and legitimate purposes. Cyber criminals might have found a new resource in the form of Aadhaar, which is linked to vital information sources such as bank accounts and mobile numbers of every Indian. It is important for authorities to be on their toes in safeguarding the same from future unknown hacking techniques.

Identity and reputation: For businesses, industries, governments, and citizens; identity and reputation are going to be everything. As such, damage due to a potential cybercrime could be significant and difficult to restore or repair. Identity theft and espionage would be a lucrative focus for cybercriminals to either launch attacks using stolen data or through direct extortion from individuals and businesses.

Cryptocurrency mining: Cryptocurrencies can be mined using computational power, and profits can be earned as arbitrage between value of coins mined and the cost of infrastructure and power. Cybercriminals can exploit private and government infrastructure by deploying malware for mining cryptocurrencies in an unauthorised manner. From one compromised server in a data centre, a hacker can easily mine $2,000 a month. This would cause loss of business, hardware damage and increased costs for the victims.

Cyber-jacking: Instead of physically hijacking a plane, cyber criminals can hack into the management systems of aircrafts and hijack or crash a plane.

Human malware: Hackers can target pacemakers, cardioverter-defibrillators, insulin pumps, and other such devices. Researchers have demonstrated that it is possible for hackers to break into your implant and cause collateral damage.

Quantum computing: High-speed computers with tremendous computing power are being developed to assist artificial intelligence applications, robotics and machine learning. The computing power of these machines can easily break the current encryption technologies and cause havoc if they get into the hands of a cyber criminal.

Industrial espionage: Cyber attacks in the future will be geared towards industries of prime importance such as power, energy, oil and nuclear power. Such attacks can disrupt the critical infrastructure of a country, especially if done through a state-sponsored platform.

Misuse of augmented and virtual reality can be exploited for frauds and social engineering attacks.

Cybercriminals of the future would be more focused, better planned, better equipped and would work in a collaborative fashion with other cyber criminals to launch more sophisticated attacks on individuals and businesses.

With advancements in digitization, organizations, individual as well as defence establishments would be potential targets of cyber criminal activities. Threats such as cyber-jacking and human malware could lead to physical injury as well as loss of life. Furthermore, there are usually multiple agencies responsible for cyber security and they may not be coordinated to match the future cyber criminal. The rise of cybercrime in the current years serves as a great signal for the incrementing societal engagement in issues of data protection and internet governance. It is assumed that citizens will demand greater transparency as well as accountability from the governments and service providers, and even some kind of data autonomy. Taking a cue from Europe's General Data Protection Regulation (GDPR), it is important for governments and businesses to understand that an individual's data is his or her asset and eventually individual's rights can be exercised under a mature regulated environment. Hence it is important for increased data protection and governance culture.

Existing laws along with the mindset of law enforcement agencies need to evolve to confront the challenges of potential cybercrimes in 2020. In addition, law-enforcement agencies need to upgrade themselves with the latest technologies such as artificial intelligence and robotics to better tackle the future cybercrime. Internet protocol (IP) address or source tracing remain a challenge due to use of proxies, virtual private networks (VPNs) or Tor relay points. A possible solution to this might be allocation of IPv6 addresses on an individual basis. IPv6 uses a 128-bit address, theoretically allowing 2^128, or approximately 3.4×10^38 addresses, which is significantly more than what is required by the human population. If every user is allocated an IPv6 address, which is required to connect to the internet, it will eliminate the issue of IP tracing. Such IP addresses can then be mapped to Aadhaar to track online communication, just like mobile telecommunication. A combination of increased user awareness and use of advanced technologies for defence will go a long way in helping individuals and enforcement agencies deal with the future of cybercrime.

Amit Jaju is partner, forensic technology and discovery services, EY India.

END