Source : www.livemint.com Date : 2018-12-20

OPINION

Relevant for: Security Related Issues | Topic: Basics of Cyber Security and related matters

The wars of the 21st century will be to capture, manipulate or destroy others' data. Digital systems powering organizations and nations around the world have become prime targets for attack—from individual criminals, well-organized cybercrime gangs, and state-sponsored hackers.

As the internet becomes all pervasive and the world gets increasingly interconnected, cyberattacks are bound to create widespread impact. The WannaCry hacking attack in May 2017 that crippled computers across 150 countries is just an example of the pervasive nature of this problem. Billions of dollars are being wasted in the destruction, downtime and replacement costs arising as a result of cyber insecurity. Cyber security—the various technologies, processes and practices that protect networks, computers and digital data from attack—is a prime focus area for all types of organizations. It is dominated by those who believe that new and more complex technology will save us from all sorts of cyber attacks. Will this approach protect our cyber world?

While building these complex and expensive technological solutions, we often forget the human beings who are at the centre of the issue. Cybersecurity teams that are mostly led by technology experts tend to see the whole problem through their technological lens. They tend to believe that the hacker is looking for technological weaknesses in their software or technology network. They are always focused on trying to correct the technical bugs in their system. Various studies and analyses of cyber attacks across the world have shown that in more than 90% of the security breaches, the enabling factor has been the negligent behaviour of users. The spread of a malicious worm that attacked the US Central Command system started with the insertion of an infected USB drive by an individual in a US military laptop. It took the Pentagon more than 14 months to clean things up.

Many cybersecurity experts harbour a false belief that hackers only focus on technological vulnerabilities. However, the truth is that human behaviour is often the weakest link in the online security chain. A large number of cyberattacks begin with a phish—a fraudulent attempt to obtain sensitive information under the guise of a trustworthy entity. Humans have a bias that gives credence to authority. So, it will be difficult for a person to ignore a phishing mail, purportedly from an authority figure. Other biases used to gain access include our almost automatic responses to reciprocity and prior commitments. These techniques employed by cyberattackers bypass the best security walls a cybersecurity team can develop.

Cybersecurity experts understand the complexity involved in detecting the flaws in a security software, rectifying it and developing a secure technological barriers to prevent any attack. Even if we understand how social hacks work, building defences is another matter altogether. Simple tasks, such as getting employees to use strong passwords, changing them frequently, or avoiding the use of unsecured public Wi-Fi, are not as easy as they appear to be. The complexity of the human brain creates several impediments in the initiation and maintenance of these tasks.

The human brain will always try to reduce the cognitive load involved in any decision. It is for no other reason that 123456 is the most common password. The human brain loves status quo. So, on being asked to change the password, the user will only want to make a minor change to the existing password. So if the old password is password1, the new password will most probably be password2.

Humans have very poor ability to evaluate risk. Various researches have shown that humans evaluate the risk involved in a particular action not based on any elaborate calculation but how one feels about the action one is taking. If one feels positive about the outcome of that decision, they are likely to judge the risk of that action to be low. So for an employee watching a movie after working for long hours, the enjoyment the movie provides far outweighs the risk involved in using an insecure USB drive.

Given a choice between the enjoyment in the immediate moment and a potential risk in future, the human brain will always have a bias for the present. Combined with our brain's tendency to discount the future, more so risks in future, most employees will have a tendency to underestimate the risk involved in their decisions.

Appropriate emotions about risks are generated when a well publicized news about a cyberattack is made available to everyone concerned. As long as the news of the event is available in one's memory, everyone will get into a cautionary mode and will follow the required security measures. However, as the memories of those incidents recede, people get complacent. Very rarely do security experts realize that a complacent mental mode an employee gets into opens up far more opportunities for a cyberattack than even a significant flaw in the software of a security system.

So while billions of dollars are being spent to take care of the technical requirement of cybersecurity, there is comparatively little investment made to understand and influence the human behaviour around cybersecurity. The sooner we realize that the most powerful technological solutions are no match for a cyberattacker with an excellent understanding of the working of the human brain, the safer our cyber world will be.

Biju Dominic is the chief executive officer of Final Mile Consulting, a behaviour architecture firm.

Comments are welcome at theirview@livemint.com

END