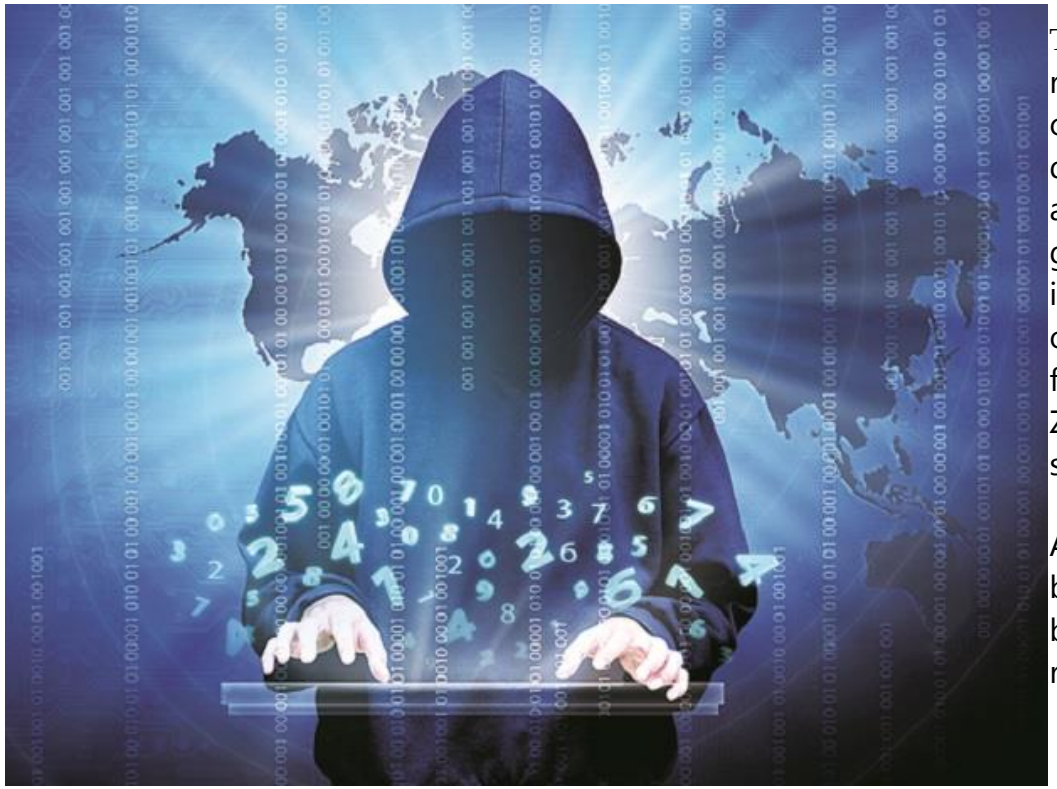
Business Standard

Dealing with the WannaCry ransomware attack

Ransomware attacks in the digital space have been around of over a decade now

Sayan Ghosal | New Delhi May 22, 2017 Last Updated at 01:07 IST http://mybs.in/2UVmK0i



The recent WannaCry ransomware attacks have rekindled the debate over India's lack of comprehensiveness in the cyber security and data protection arena. With over 200,000 attacks affecting a variety of commercial entities globally, cyber experts are terming this infringement as a 'wake-up call'. Amid reports of personal data theft of around 17 million users from the database of the food-delivery app Zomato, these events have once again put the spotlight on the issue of data security.

Although India seems to have been spared the brunt of the WannaCry attacks, this may be because of the country's low standards of reporting such cyber crimes.

Ransomware attacks in the digital space have been around of over a decade now, with the first documented case dating back to 2005 in the US. In fact, the Indian Computer Emergency Response Team (CERT-In), a nodal agency that deals with threats to cyber security, had issued a critical warning in this regard in April this year. Businesses were advised to ramp up security measures and report instances of data breach — which was made mandatory after a government notification earlier this year.

According to Rahul Sharma, senior consultant, Data Security Council of India, reporting to CERT-In allows organisations access to experts and also helps the agency to analyse multiple variants of such attacks. Affected entities can also reach out to cyber Section 43: Penalty and compensation for damage to computer, computer systems, etc. Section 43A: Compensation for failure to protect data Section 65: Tampering with computer source documents — imprisonment up to 3 years and/or fine up to ~2 lakh Section 66: Computer-related offences — imprisonment up to 3 years and/or fine up to ~5 lakh Section 66F: Punishment for cyber terrorism — Up to life imprisonment crime investigation cells, but bringing these criminals to task is difficult, given the transnational nature of such attacks.

Under the Information Technology Act, 2000 (IT Act, 2000), companies have the responsibility to protect 'sensitive personal data or information' (SPDI) of consumers. "According to Section 79 of the IT Act, each entity is obligated to take all reasonable care and observe due diligence while discharging its duties," says **Salman Waris, partner, TechLegis**.

Section 43A of the Act also says that a company might be liable to pay compensation for losses caused due to negligence in implementing and maintaining reasonable security practices and procedures. The IT Rules, 2011, say these security requirements must conform to international standards or comparable standards notified by the government.

According to Sharma, though there are certain risks that are beyond organisational control, the non-patching of systems with requisite security updates released in the public domain is inexcusable. "If this (WannaCry ransomware) attack exposes the inability of organisations to protect SPDI, they are liable to pay compensation to individuals," adds Sharma.

As a result, companies affected by these events should focus on collecting forensic evidence to help in investigations and defend themselves against consumer claims. *According to Waris these entities may also need to show that they have implemented security control measures in accordance with their security programmes and policies*.

Apart from protecting themselves in the short run, companies must also adopt the latest software and security measures to ensure they keep themselves protected from such attacks. These include implementing data isolation techniques and backing up sensitive data — which is a requirement under Section 76C of the IT Act.

Conducting frequent cyber security audits — at least once every year — and regular cyber vulnerability assessments will also help bring Indian cyber security standards on a par with countries like the US, Germany and China.

Citing the Nasscom India data, Waris says that India spends only 0.8 per cent of its web expenditure on data security. *"Generally, there is only a knee-jerk reaction to data thefts or high-profile breaches that force corporates to act in this regard,"* he added. Experts note that companies must shift from viewing security spends as cost centres and start looking at them as business enablers. "Such a massive global outbreak also warrants international collaboration and a collective response to book cyber criminals," adds Sharma.

Progress on the National Cyber Security Policy — first drafted in 2013 — and the proper enforcement of reasonable security practices will also aid in creating a stronger cyber safety framework. As always, vigilance and preparedness will be the key to securing India's cyber space.