Strangulating Cybercriminals – Ways and Means

BY ROBIN BANERJEE, AUTHOR, CORPORATE FRAUDS

British Airways which once boasted to be “the world’s favourite airlines”, invited its customers’ ire, when personal data of 400,000 people got stolen by hackers in the summer of 2018 including their credit-card details. The airlines was imposed a heavy fine of £20 million for the data breach. But what really peeved the customers was the reaction of the management which refused to take unconditional responsibility for the breach. This unacceptable attitude impacted the reputation of BA’s brand. Every company management is expected to ensure cybersecurity. Unfortunately, some top managements do not take this responsibility seriously. In the modern world, the ability of entrepreneurs to manage cyber risk has far-reaching implications for corporate goodwill, stock prices and professional reputations.

PRECAUTIONARY FOOTSTEPS:
Companies need to adopt the following defences against the cyber fraudsters:
• Proactive health-check: Businesses must attempt to carry out proactive rather than reactive digital-health checks.
• Enhanced awareness: A heightened perception of both personal and collective liability of the management, helps.
• Make fraud-security inclusive: Companies should work to make fraud security a ‘business as usual’ process by training employees and implementing a security policy.
• Adopt the best practice: Most measures for controlling digital frauds could be outdated. Hence organizations should aim to implement internationally-recognized standards of best practice.
• Put in a back-up plan: Companies should put in place contingency or disaster recovery plans. Should an untoward incident occur, it is in a position to respond efficiently to minimize any disruption to the business.
• Cyber-insurance policy: Cybercrime risks are insurable. Such policies have become more comprehensive and cover more than they did earlier. Negotiate one before the ghost strikes, and not in the midst of the episode. It should normally cover most costs associated with a data breach like counsels to guide you, forensic firm to unravel mischiefs and even a ransom that the company could pay to get its data unencrypted.

QUICK SIXER ACTION-PLAN
‘Take-five’ is a campaign being run by a financial trade association ‘UK-Finance’ and the UK-Government, to popularise simple steps to avoid cyber frauds. Drawing inspiration from it, I give below my ‘adopt-sixer’ steps, which are all common sense. Regrettably, it is uncommon to have common-sense which lends many of us to be scammed.

1. Beware that a genuine bank or organization will never contact you out of the blue to ask for your PIN, full password or to move money to another account;
2. Use a strong password which is not easy to guess and not to use same password for all accounts. Use hard to guess but easy to remember password. You may use password manager to remember passwords.
3. Never transfer money to any unknown account;
4. Do not be tricked into giving a trickster access to your personal or financial details;
5. Always question uninvited approaches; instead, contact the company or vendor directly;
6. Never answer or act upon any e mail or phone calls announcing too good to be true offers and then give your personal information, howsoever sketchy it could be to start with.

The best way perhaps for organizations to reduce the risk from cybercriminals and prevent external hacking, is to understand a hacker’s mind-set. Corporates need to think like a hacker to comprehend their actions, anticipate and confront them. Hackers usually are skilled, intelligent and risk takers, waiting to exploit a vulnerability in the system to break in. They are mostly great actors and communicators, capable of manipulating people’s psychology to part with crucial data and perform desired actions. You need a hacker’s mentality to hack the hacker’s habits!