

Making the best of hacking

What do you do with a schoolboy who is mischievous and incorrigible? Make him the school leader. How do you treat an employee who revolts against the management and mobilizes others in his mission? Make him the manager. By the same logic how do you punish a hacker who breaches your network security? Make him your company's network strategist! Yes, this is precisely what some companies in the US are doing today. Realizing the futility of fighting the Net violators, companies have joined force with them. International competition to identify the best hacker held recently at New York endeavored to achieve the same.

It is a known fact that those who dare to violate are smarter than those who toil to create the same. And it is also common knowledge that those who break the rules are the ones who know the rules the best. These are the virtues that companies are trying to cash in by employing hackers as network strategists. But does it mean that companies are willingly rendering themselves vulnerable for network attacks? Will hackers really give up their passion for breaking into other networks? These are some hard questions.

Hacking itself is not a derogatory word; it is another thing that it has picked up derogatory connotations of late. The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.

Hacking, according to popular perception is unauthorized use of computer and network resources. But the hacker community looks at it in a different light. It considers hacking a celebration of knowledge, inquisitiveness and freedom. As per them hacking is to seek knowledge, discover something new, be the first one to find a particular weakness in a computer system or simply put asking a lot of questions and refusing to stop asking. Hackers theory of hacking is not restricted to computer alone but believes anyone with an inquisitive mind, a sense of adventure and strong beliefs in free speech has a bit of the hacker spirit in them. Anyone who's an adventurer or explorer of some sort, or any good investigative journalist, knows the feeling of wanting to do something nobody has ever done before.

Hackers are considered to be a great threat because of their disassociation with the powers that be. Since most of the hackers operate in isolation and do not have an organized approach to things, they pose a great danger to organizations. But it's interesting to note that hackers are the ones who push for stronger encryption and help companies to stay secure unlike some other forces that try to weaken encryption. Even system specialists acknowledge the usefulness of hackers in securing enterprise systems. According to IBM Consulting, when hacking is done by request and under a contract between an ethical hacker and an organization where the ethical hacker has authorization to probe the target, it is considered legal. This effectively wards off the common misconception that all hacking is illegal.

All said and done hackers would continue to be destructive unless their creative abilities are channeled properly. Being a reformed hacker helps, but as the hacker community itself admits, the hacker then no longer carries that urge to explore the unknown. He becomes a willing accomplice in furthering organizational growth within the 'parameters' of that organization. Nevertheless companies need to take hackers into their fold instead of alienating them.

G.P.Vinaybabu
vinayg@mm.strategicnewspapers.com
E-SECURE- September 2000