Cyber Security

How hackers can be a force for corporate good

Rewarding security researchers for finding bugs is vital in the connected world

Keren Elazari

A US team of hackers competes against 17 other nations at the Seccon 2015 competition © AFP

APRIL 10, 2017 by: Keren Elazari

The upshot of the information age is that "software is eating the world". In a rush to create digital code and services, companies competing to be the first to market do not prioritise cyber security — even though security problems and software bugs are a known certainty. When even secure organisations experience data breaches and security incidents, it is clear they need all the help they can get.

Surprisingly, software giants now encourage hackers to hack them. Companies such as Google, Microsoft and Facebook have been doing this since 2010, in what are called "vulnerability reward programmes", or more commonly "bug bounty programmes". In an echo of the American wild west, companies offer independent security researchers the chance to win rewards and recognition for identifying critical security problems — software vulnerabilities that could put us all at risk.

While 2016 may have been "the year of the hack", including the huge denial-of-service internet outage in the US in October, 2017 could be "the year of the friendly hack". There are more bug bounty programmes in traditional industries, outside Silicon Valley. MasterCard, Johnson & Johnson and even the Pentagon are inviting hackers to work with them and test their systems for vulnerabilities. By rewarding hackers for their discoveries, these organisations can learn from their findings, prevent security breaches, and even recruit top cyber security talent.

This explains why leading companies are willing to pay out millions of dollars in rewards. According to Bugcrowd, which manages many programmes for other companies, in the past few years Google, Facebook, Yahoo, Microsoft and Mozilla paid friendly hackers a total of more than $13m in bounties.

The idea of a bug bounty is not new: in 1995 Netscape offered rewards to users who found bugs in the trailblazing Navigator 2.0 web browser. Now, thousands of ethical hackers help hundreds of organisations find software bugs, using the power of many to make us all safer. Rewards range from T-shirts to 1m airline miles or a $200,000 single reward that Apple offers for certain discoveries.

Bug bounties are becoming more widely accepted because the benefits they provide can greatly outweigh the risks: never before has it been so easy for hackers to legitimately report findings to the companies affected by them and get rewarded without breaking the law — a hacker-specific take on the "gig economy", if you will. It is also a cost-effective way to find security bugs for the companies in question, as empirical economic research has proven.

Some of the best bug hunters end up being offered full-time corporate positions. These are hackers from all over the world, whose location, access to college education or finances may never have afforded them the chance of an interview — with the result that companies would have missed out on their incredible talent.

The latest corporate benefit, one suggested by the Berkeley Technology Law Journal, is that bug bounty programmes can become a corporate governance "best practice" mechanism. Having such programmes in place can help directors exercise their "duty to monitor" digital assets.

Finally, you might ask: won't criminals take advantage of these programmes? The truth is they seldom require an incentive to hack. They are already at it, making millions illegally. These programmes allow individuals who spot a problem to do the right thing and give companies a chance to sort it out, while getting legitimate payment and recognition. The process represents a practical way to harness the impact of thousands of security researchers who are helping to build a much-needed "immune system" for our connected age. That gives me hope.

The writer is a senior researcher at Tel Aviv University Interdisciplinary Cyber Research Centre and a strategic analyst