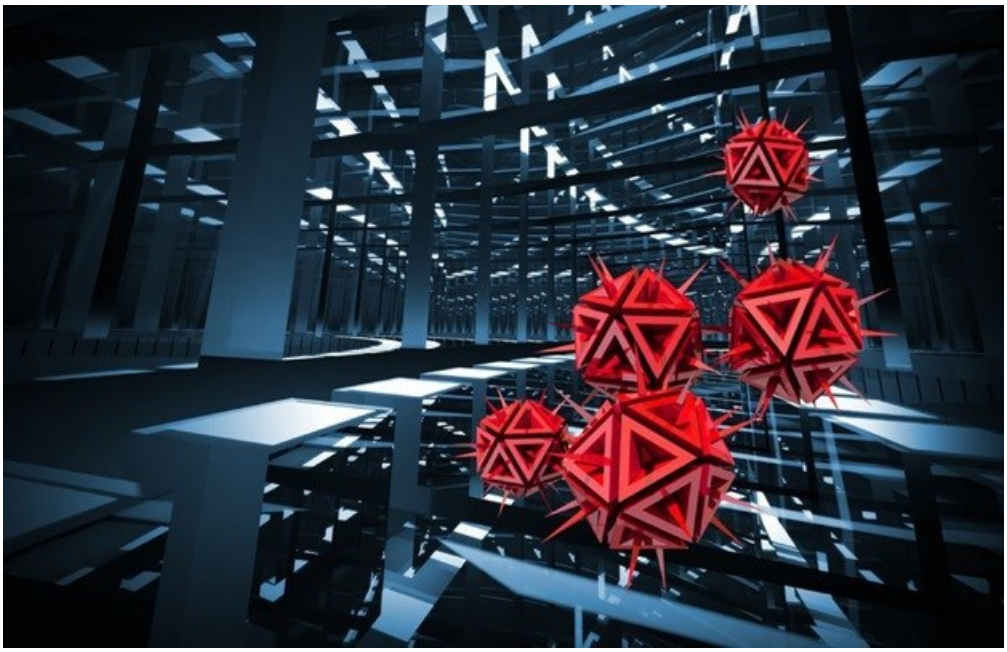
BIZCOMMUNITY

There's a massive cybersecurity job gap - we should fill it by employing hackers

By John McAlaney and Helen Thackray

24 Apr 2019

Cybersecurity incidents are gaining an increasingly high profile. In the past, these incidents may have been perceived primarily as a somewhat distant issue for organisations such as banks to deal with. But recent attacks such as the 2017 Wannacry incident, in which a cyber attack disabled the IT systems of many organisations including the NHS, demonstrates the real-life consequences that cyber attacks can have.



These attacks are becoming increasingly sophisticated, using psychological manipulation as well as technology. Examples of this include phishing emails, some of which can be extremely convincing and credible. Such phishing emails have led to cybersecurity breaches at even the largest of technology companies, including Facebook and Google.

To face these challenges, society needs cybersecurity professionals who can protect systems and mitigate damage. Yet the demand for qualified cybersecurity practitioners has quickly outpaced the supply, with three million unfilled cybersecurity posts worldwide.

So it might come as a surprise that there is already an active population with a strong passion for cybersecurity – hackers. This is a term with many negative connotations. It evokes the stereotypical image of a teenage boy sat in a dark room, typing furiously as green text flies past on the computer monitor, often with the assumption that some criminal activity is taking place. The idea of including such individuals in helping build and protect cyber systems may seem counterintuitive.

But, as we have highlighted in our recent research, the reality of hacking communities is more complex and nuanced than the stereotypes would suggest. Even the phrase “hacker” is contentious for many individuals who may be labelled hackers. This is because it has lost the original meaning: of someone who uses technology to solve a problem in an innovative manner.

Researching cyber security. Bournemouth University, Author provided

Hacking today

There are a growing number of online hacking communities – and regular offline meetings and conventions where hackers meet in person. One of the largest of these events is DEFCON, held every year in Las Vegas and attended by up to 20,000 people. These hacking communities and events are an important source of information for young people who are becoming involved in hacking, and may be the first contact they have with other hackers.

On the surface, the conversations that are held on these forums often relate to sharing information. People seek advice on how to overcome different technical barriers in the hacking process. Assistance is given to those who are having difficulties – provided that they firstly demonstrate a willingness to learn. This reflects one of the characteristics of hacking communities, in that there is a culture of individuals demonstrating passion and the desire to overcome barriers.

But such events are about more than sharing practical skills. As individuals, we are strongly influenced by those around us, often to a greater degree than we are aware of. This is especially the case when we are in a new environment and unsure of the social norms of the group. As such, these online and offline hacking communities also provide an important source of social identity to individuals. They learn what is and what is not acceptable behaviour, including the ethics and legality of hacking.

Technological approaches alone cannot prevent cyber attacks. Bournemouth University, Author provided

Myths and opportunities

It is important to stress here that hacking is not an inherently illegal activity. There are many opportunities to engage in ethical hacking, which refers to attempting to hack systems for the purpose of finding and fixing the flaws that malicious hackers may try to exploit for criminal activity.

Our research demonstrates that the majority of people active within hacking communities have no wish to exploit the flaws they find although they do believe that such flaws should be exposed so that they can be addressed – especially when the organisation concerned is holding public data and have sufficient resources that it is reasonable to feel they should not have any gaps in their cybersecurity in the first place. Several large and well-known companies actively engage with this culture, by offering hackers "bug bounties" – financial rewards for identifying and reporting previously undiscovered weaknesses in their systems.

Of course criminal hacking does happen – and many of the people we have spoken to acknowledge that they take part in activities that are of questionable legality in order to achieve their goal of finding the flaws in a system. This creates a risk for those people, especially young adults, who are becoming involved in hacking. Through ignorance or through being wilfully misled, they may become involved in activities that result in them gaining a criminal record.

If so, this impacts not only them as an individual but also the cybersecurity profession. As a result of this culture, many companies are being deprived of individuals who could have helped fill the increasingly urgent gap in cybersecurity professionals. To address both of these problems, we need to move past unhelpful and negative stereotypes and work with young people and hacking communities to provide an awareness of how their passion and skills can be used to address the cybersecurity challenges that society faces.

ABOUT THE AUTHOR

John McAlaney, associate professor in psychology, Bournemouth University. Helen Thackray, senior research associate, University of Portsmouth.