Bounties for bug-hunters make the internet safer

HackerOne's network of more than 100,000 ethical hackers can help online organisations eradicate vulnerabilities in their internet systems that could be exploited by criminals, says Mårten Mickos, its Chief Executive Officer

Barely a month goes by without reports of large companies and government bodies suffering cyber-attacks by criminal hackers and other hostile organisations. A USD92 billion cyber-security industry has grown up which tries to fend off such attacks by building walls and gates. But such strategies are easily outpaced by hackers – frequently proving inadequate and undermining the confidence of online users.

However, a California-based company has developed a revolutionary new approach that invites ethical hackers to detect vulnerabilities in the computer systems of its clients. HackerOne, founded in 2012, has already attracted more than 1,000 companies, including well-known dotcom businesses such as Twitter, Yahoo!, AirBnB and Uber. Its bug-hunters, who now number more than 100,000, are paid bounties for their successes – and more than 4,000 have already shared USD14 million for finding over 28,000 vulnerabilities.

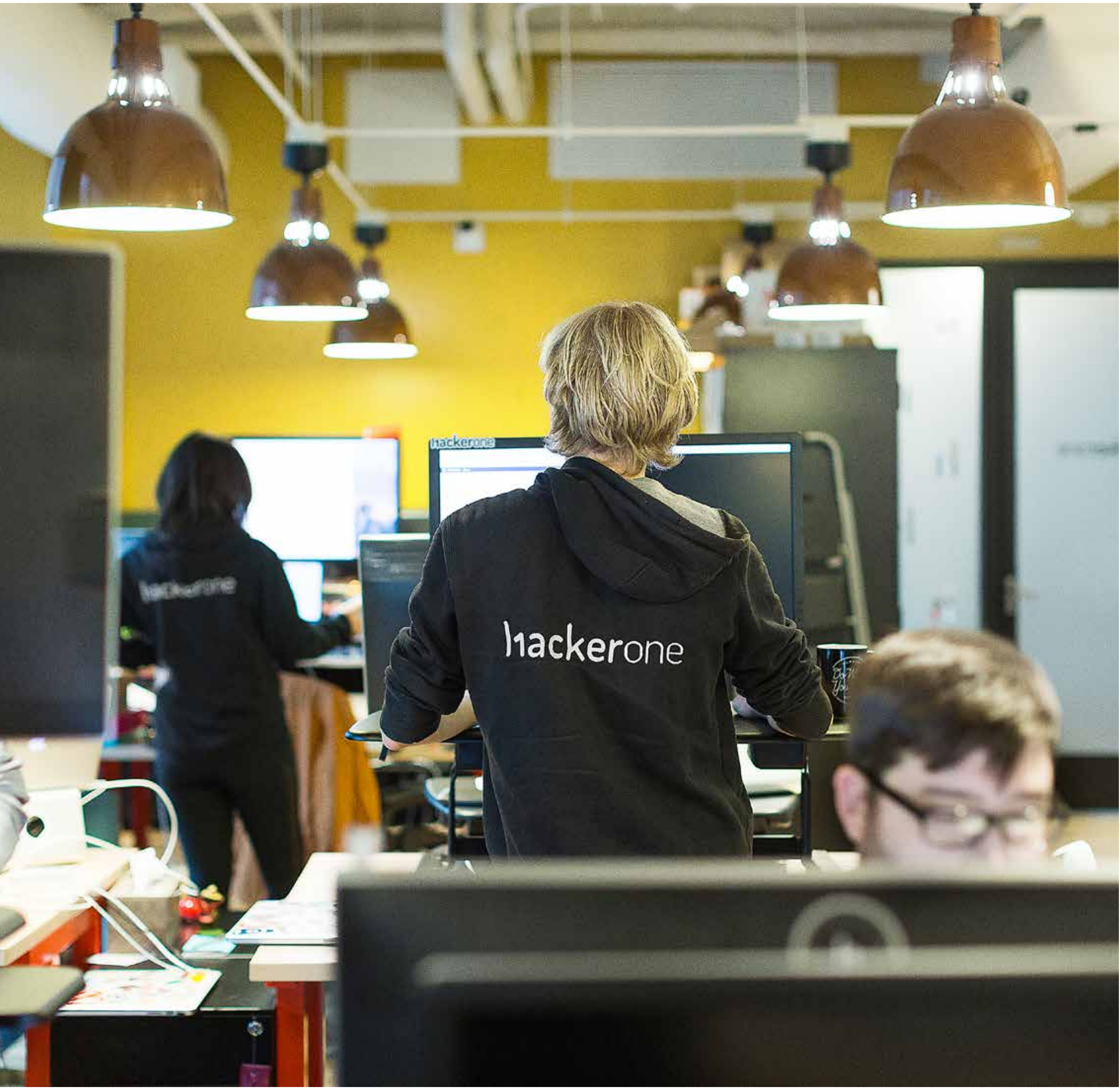
When Mårten Mickos was approached to become HackerOne's CEO in 2015, he was at first sceptical of joining: he saw the cyber-security industry as rather cynical and negative. But when he met the founders, he found it to be a positive and constructive company which offered an enormous opportunity to build a society that could function safely and securely online.

'We're trying to turn security inside out, based on a principle which has existed for a long time,' he says. 'We're asking people to help by looking in, rather than building barriers to keep them out. It's like Neighbourhood Watch schemes which encourage people to keep an eye on their neighbours' homes when they're on holiday, to stop them being burgled.

'We are a trading platform that brings together responsible 'white-hat' hackers with responsible companies in order to make the connected world more secure. Our hackers are independent operators who are paid by our clients for the vulnerabilities they discover. We encourage clients to share on our website what our hackers have found so that others learn from their experience – which around 10 per cent do.

'We have more hacking experts than any other company in the sector and they are diverse in their backgrounds – young and old, men and women, technical and non-technical people. This makes us

‘We’re asking people to help by looking in, rather than building barriers to keep them out’



better at finding vulnerabilities than the limited number of in-house experts working for client companies. And it is hard for humans to find flaws in the systems they have built; creative outsiders are more likely to find the "unknown unknowns" – vulnerabilities that no-one else has spotted.'

HackerOne's typical hacker is a young man under 34 with expertise in computer sciences, for whom detecting online flaws is a hobby at college or a spare-time job. They have a cunning ability to think bad like a criminal hacker, says Mårten Mickos, but then do good by reporting the vulnerabilities to the owner of the system – the potential victim. They find chasing vulnerabilities thrilling and they can make a lot of money if they're good – one of HackerOne's bug-hunters made over half a million dollars on the HackerOne platform alone.

'I see us as a bit like the Boy Scouts, whose founder created the organisation as a way of giving idle young people something to do and contributing to society. Often our hackers are super-intelligent teenagers who don't know how to communicate with people and may be difficult to deal with. We reach out to them, giving them a meaningful role in society and bringing out the best in them – otherwise they might get up to all sorts of mischief.'

HackerOne's approach has proved attractive to a wide variety of companies. Those which have grown up in online businesses such as Uber and AirBnB know that constantly detecting vulnerabilities is vital to their success. Older companies which have experienced their first security breach, perhaps by a criminal, quickly turn to us because they cannot afford the cost of another breach. A third group of clients comes by recommendation, often from big manufacturing companies which tell their suppliers to protect themselves against hacking so as to make the supply chain secure.

In 2016, HackerOne helped the US Department of Defense to make its systems more secure by launching the 'Hack the Pentagon' challenge.

'We have more hacking experts than any other company in the sector and they are diverse in their backgrounds'

This eight-week programme involved 1,410 hackers who found 138 vulnerabilities – the first within 13 minutes. It paid out USD75,000 of bounties to the hackers, ranging from about USD100 to USD15,000.

'It was a huge shock for the Pentagon to find so many flaws, having previously paid millions of dollars on security protection. So they asked us to repeat the programme for the US Army with Hack the Army, and again found very serious vulnerabilities – the first within five minutes. The Department of Defense is one of the best financed organisations in the world which can pay for anything it needs, but it found it effective to turn to hackers for help!'

Big online operators often pay for continuing surveillance, while others prefer sporadic scrutiny when they launch new software. But monitoring needs to be continuous, says Mårten Mickos. 'You can't know when malicious hackers will find a flaw, as systems are under attack all the time from criminals, hacktivists, nation states and terrorists.'

The most common bugs are considered 'low-hang - ing fruit', he adds. Cross-site scripting (XSS) vulnerability allows hackers to get access to content on another website, for example. The most severe attacks include attackers putting software code on a system which can stop it operating or steal its data. 'Every day, we spot new vulnerabilities which our customers must get their engineers to fix.'

Particularly vulnerable are users of old software which may have been designed before anybody thought about cyber-security, and those whose security practices have not been kept not up-to-date. Organisations that do not pay attention to cyber-security in their operations are also vulnerable, and need to change their cultures. The best online companies put security at the heart of their organisations, treating it as an integral part of the corporate life-cycle.

The growing threat posed by serious hacking leads to worries that the internet is too open, and that users will move into more closed forms of online communication. But Mårten Mickos says that vulnerabilities can be greatly reduced – as happened with previous technological innovations which experienced safety issues in their early days.

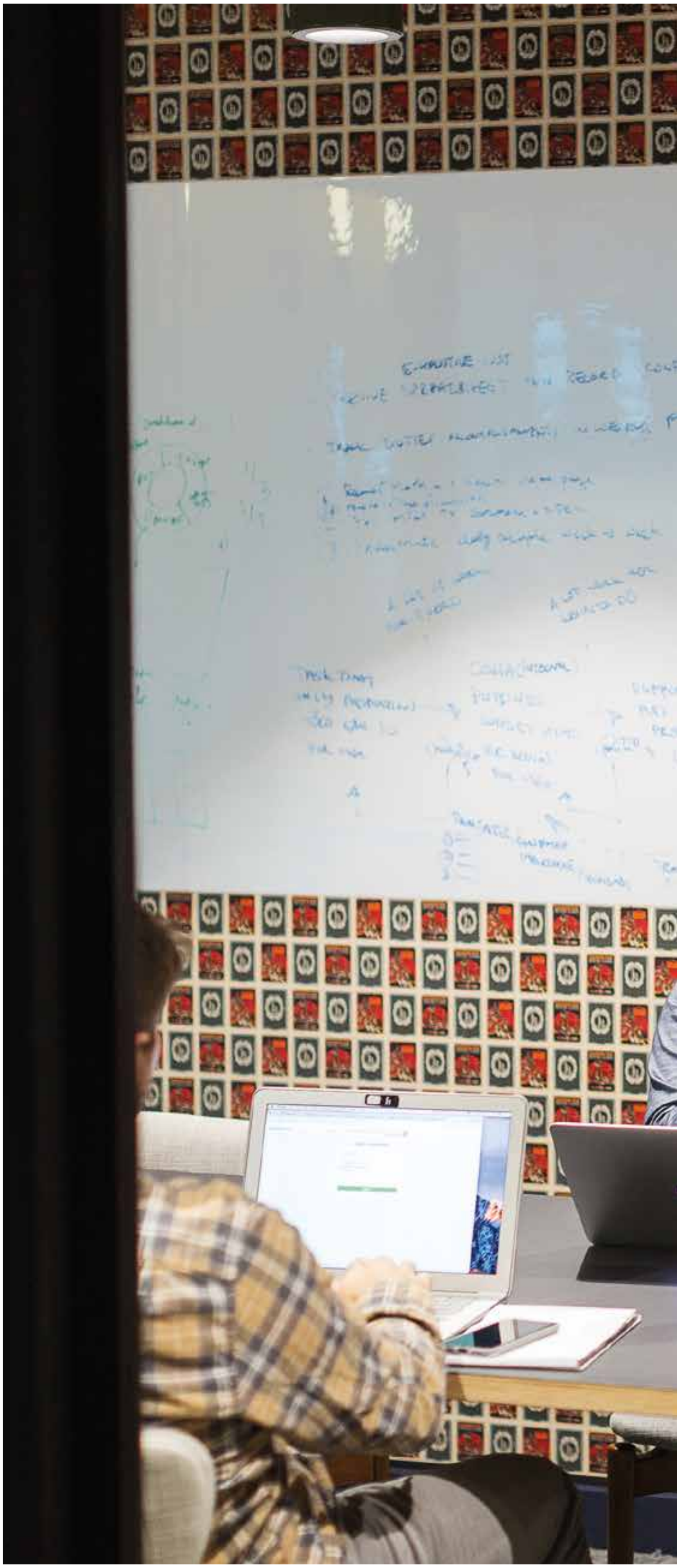
‘There is no 100 per cent safety in cyber-security’

‘When cars were first made, manufacturers didn’t think about security and people died all the time in accidents. When the auto industry decided to make security a priority, it started to build safety into every car. People still die in traffic, not because cars are unsafe but mostly because of their owners’ driving practices. The same will happen with software, an industry that is only 30 years old. More companies will design security into their products and create a society where software is truly secure.

‘There is no 100 per cent safety in cyber-security but we can get closer to it – just as happens with infectious diseases which have been reduced by vaccinations and better hygiene. There will remain parts of the world where cyber-security is inferior to best practice, but in advanced societies the internet will become much more secure over time.’●

How Mårten Miskos protects his own security online

– Change passwords frequently and make them cryptic
– Back up data at all times
– Treat every communication as being from a potential attacker – even if apparently from a friend or colleague, it could be a phishing attack searching for a vulnerability in your security defences
– Don’t respond to cold calls by telephone unless there is independent and reliable proof of the caller’s identity
– Don’t allow strangers to use your phone or tablet, however good the reason
– Make security a habit, not a burden – and don’t stop enjoying your connected life



- Inbox: * Sort by severity
* custom view ?
(default views)
- Filter by severity
bugs view
hacktivity
- Severity on Dashboard
- Integrations
* slack
* Report escalation
Impact Reputation
- Bounty Recommendation to use severity data.
- Severity on Hacker Profile
- badges "Big Game Hunter"
5 critical resolved
severity combined w/ CWE
Severity into hacktivity weights
structured
=> vulnerability taxonomy
Spiced ~~Apple~~ Cats Cider