Train Your Employees to Think Like Hackers

By: Mårten Mickos, CEO, HackerOne

Harvard Business Review

hackerone

Companies that want to help their employees become better stewards of cybersecurity need to go beyond regular trainings on password security and other basic protocols. **The best way to train employees to defend against hackers is to teach them how to think like one. The first step is getting smart about what it actually means to be a "hacker."**

Start by forgetting everything the media and entertainment industry has told you about hackers. The media has a history of sensationalizing the term by using it to denote cybercriminals. This is too narrow a view.

In many ways, hackers are the model citizens of the digital era. They are creative, persistent, and resourceful. They think in digital terms and have the curiosity and drive to figure out how technology works. They view every problem as an opportunity. They stand up for what they believe in and they want the world to be a safer place.

Hackers also know a thing or two about the limits of technology. They have a healthy mistrust of computer systems and they understand that no software is immune to bugs (and that even without bugs, software will still have security vulnerabilities). They also know that just because computers and software can do a lot of good, it doesn't mean they can't also be used for doing a lot of bad. To them, it goes without saying that software will always do MORE than it was intended to do, and so they are constantly on the lookout for vulnerabilities.

For those of us who were born before the digitalization of society (probably the majority of your workforce), these concepts may sound foreign. But for hackers, it's simply the way the world works — and they're right.

That's why it's so important for companies to start cultivating the hacker mindset inside their own organization today. Not only can it change the way employees view and value cybersecurity, which leads to better security across the entire organization, but it can also help your workforce become more curious and resourceful — two of the most valuable skills in a future with widespread artificial intelligence and automation.

Here are a few ways companies of any size can start teaching their workforce to think like hackers:

Hackathons and Competitions

Encourage employees to attend hackathons — even if only perhaps to observe or learn. These events give people a chance to take a step back from their day-to-day work for a moment and think creatively to solve some kind of problem, which is what "hacking" is all about.

Sometimes these events are related to the product or business, but they can also be focused around something else entirely. The idea is to get people shifting gears and exercising their mental muscles in new ways. This helps teams avoid tunnel vision and groupthink, and gets them thinking more creatively. It also makes everyone more observant and curious about the world around them, which is at the very heart of good cyber hygiene.

For more hands-on cybersecurity learning, arrange company-wide competitions and games that encourage employees to figure out how cybercrime could potentially happen. You can even take it a step further and role play a fictitious cyber incident. Acting out a breach scenario can help employees, technical or not, better relate to organizational risk and inspire a new level of mindfulness when it comes to cybersecurity.

Incident and Information Sharing

When something major happens in your industry, encourage teams to share findings and analysis. That's not to say everyone needs to be writing up ten page reports — a few quick thoughts will do. The idea is to condition your workforce to make it second nature to share information and insights.

When you break down the silos that exist across teams in so many companies today, it helps build community and create a shared purpose, which are powerful defenses when it comes to cybersecurity. It helps create a more vigilant workforce that is more likely to detect and respond to threats.

This is especially important with security teams. When there's an incident, they should debrief a broader group on what happened and how they responded. If vulnerabilities are found and fixed, they should work with the software architects, designers, and engineers to help them avoid making similar mistakes in the future. When industries are hit by major cyberattacks (like WannaCry) or vulnerabilities (like Heartbleed), the security team should actively circulate updates and information with the entire company and also host open Q&As for those who want to learn more.teams in so many companies today, it helps build community and create a shared purpose, which are powerful defenses when it comes to cybersecurity. It helps create a more vigilant workforce that is more likely to detect and respond to threats.

Teaming Up

Create a mandate for employees to work across departments and teams. This helps open up better lines of communication across the entire organization and also helps teams solve all sorts of challenges with a fresh perspective.

Even if your security team is the best in the business, the reality is that all humans are fallible. When the same people are looking at the same codebase or dashboard every day, it's only a matter of time before something important gets overlooked. That's why the most security-conscious organizations look for help outside of themselves — i.e. inviting talented and trusted outside security experts to help identify vulnerabilities.

They also keep internal security and product teams coordinating closely as new products and features are developed. While some vulnerabilities are caused by deficiencies in the code, others result from hidden functionality that is there by design. Bringing the security team into the process early can help uncover and resolve these would-be issues before they become real vulnerabilities.

Looking to the years and decades ahead, we must all learn to think like hackers. When you adopt a hacker mindset, you aren't traumatized by rapid advances in computer technology. Instead, you embrace them and recognize their ability to make the world a better and safer place. **That's not just good for security — it's good for business.**

Mårten Mickos is the CEO of HackerOne. Previously, Marten served as CEO at Eucalyptus, a cloud software company acquired by HP where he then served as the SVP of the cloud division. Before that, he was CEO of MySQL, an open-source database company acquired by Sun Microsystems. At Sun, he served as SVP of the database division.