Matthew Pardo, Contributing Writer

**Austin Business Journal**
**March 7, 2017**

# 5 reasons Austin businesses should hire 'good' hackers

Popular media is rife with references to ransomware attacks or breaches and the attackers, often referred to as hackers, behind them. What isn't usually made clear in those portrayals is that not all hackers are the immoral, dark-side villains we love to hate: the black hats.

Hackers are typically curious about how things work and how they can be tweaked to work in new and unexpected ways. They are motivated to explore the limits of systems and how far they can be pushed before they break. The good hackers — white hats — are interested in learning, teaching, helping and protecting people and systems.

The good news is that there are many more white-hat hackers than there are black hats. In fact, smart organizations hire these white hats to assess security gaps.

Here are five reasons every organization should consider working with a hacker to help strengthen their business:

1. **Get a new view:** A hacker looks with different eyes at desktops, systems, networks, processes, peoples and cultures. This alternative view affords you a glimpse into where there are exploitable gaps and weaknesses. Sure, you can buy a yearly penetration test — and you should — but having an on staff hacker provides a deeper and longer view into your organization's vulnerabilities.
2. **Take your internal team to the next level:** Every IT support person is considered a member of what is called a blue team, which does its best to defend the organization. But because they are trained on specific tools and methods, it's easy for them to believe they are covered if they don't see any red flags. A hacker will help them learn where their specific tools and processes fail. They can also devise realistic practice opportunities for the blue team through internal tests and hackathons. Working with a hacker can elevate your defenders' effectiveness.
3. **Be proactive:** A hacker understands more about the varied ways your network can fall prey to attacks, which means they can prepare more creative defenses for protecting your organization. They can take you beyond the standard security measures.
4. **Keep up with the threat landscape:** Hackers have accrued a vast amount of specialized security knowledge. Their love of learning, passion for security and interest in how systems are compromised drives them to keep up with the most current threats. This means they have a keen eye for infrastructure risks and how to reduce them.
5. **Attackers can defend, too:** In the event of an attack or breach, a hacker can assist in creative ways. They can help both the blue team to defend and the incident response team

to uncover things they might miss. Their unique view of what's possible will speed your organization's handling of incidents.

Bonus tip: If you can't hire a hacker or don't know one you trust, grow your own. Poll your team to see who is interested in learning these skills. Ensure your choice is deeply curious and loves to learn. Then give them the time and resources they need to learn the techniques that hackers know. Self-study through books and videos can be augmented with time spent in trainings, like SANS Pen Test Austin which takes place in March. Allow them time to get involved in the Austin security community, which is one of the best in the country. They can benefit from groups like the Austin Hackers Association, local security conferences including BSides Austin and Lascon, and hands-on competitions such as SANS NetWars.

As Sun Tzu said, "If you know the enemy and you know yourself, you need not fear the result of a hundred battles." Hire a hacker and move closer to knowing the enemy.

*Matthew Pardo is a web application security support engineer in Austin for Rapid7, a maker of security data and analytics software. He is also the director of education for the local chapter of Open Web Application Security Project, a global community that drives the visibility and evolution in the safety and security of the world's software.*