The Changing Workforce: Automation & the Role of Ex-Hackers

With cyber defenses succumbing to a dizzying array of attack vectors and new techniques, the security professionals fighting the battles of 21st century cyber wars will look and think a lot differently than those of the past. Orchestrating automation will become the name of the game as the battle of the bots begins, and alliances will be forged with former enemies as organizations seek to heed the lessons of prior cyber assailants. All of this will influence the talent acquisition strategies of security leaders and change the composition of the 21st century security professional for good.

Automating the front lines.

According to Radware's *Security and the C-Suite: Threats and Opportunities Report*, 40% of 200 C-level security executives surveyed stated they've had an automated security model in place for more than two years. Another 35% said they've implemented an automated model within the last two years. And just one-quarter have yet to do so.

Given the changing nature of security threats—as well as ever-strengthening solution capabilities—the shift toward greater automation is well founded. No one would assert that the design, caretaking or break-fix of information security will ever be fully automated. In fact, it's advisable to invest in quality talent to develop and evolve an organization's security strategy.

Even so, the “front lines” of attack mitigation is going the way of automation. In fact, bots are already taking over a significant portion of network and application security, compliance, cyber-attack mitigation, incident response, disaster recovery, and identity and access management activities. After all, unlike humans, bots don’t need to sleep or eat—and they rarely make mistakes. This forces companies to think differently about how they structure their security resources, keeping the human talent at the top of the pyramid and the bot armies on the front lines fighting attacks.

Security Measures

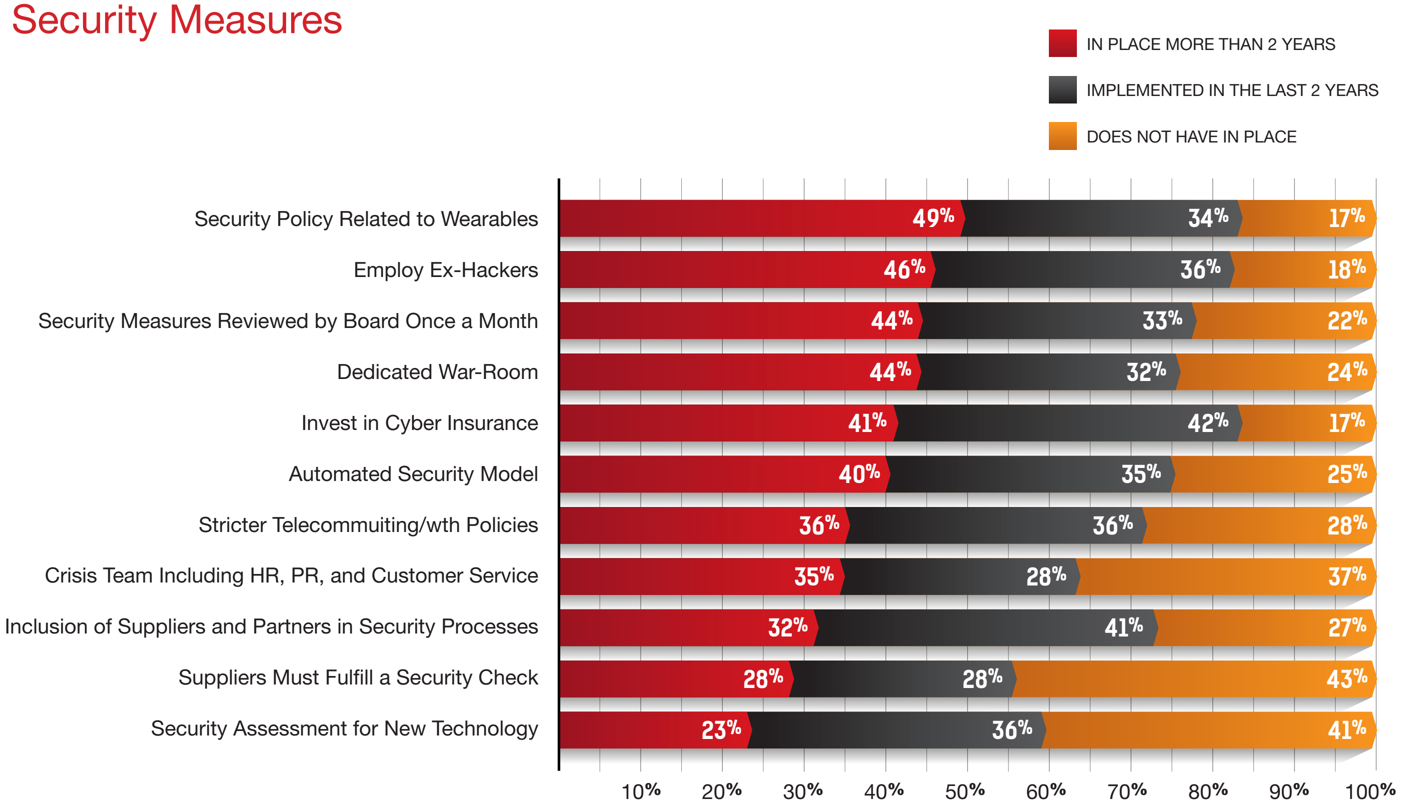

Figure 1: Security Measures

Keep Your Friends Close, Your Enemies Closer

Historically, there’s been some disagreement about the wisdom of using ex-hackers to help test networks and identify vulnerabilities. There’s obvious risk in hiring someone who has made a name for himself or herself as a hacker, as these individuals have demonstrated a willingness and ability to break the law. How can a company be certain that a former hacker won’t continue criminal behavior once inside the organization?

Executives were quick to acknowledge employee-related internal risks—risks that are only compounded when viewed through the lens of having former hackers on the payroll:

- “Insider attacks because we can’t do much to prevent it.”
- “Internal staff compromise. We hire more and more Eastern European staff that may be vulnerable.”
- “Home-based work. Too easy to hack.”

Yet, the findings of the Radware Executive Report indicate that the practice of hiring former “bad guys” is becoming mainstream. A growing number of organizations are willing to assume the risks in order to capture the potential rewards—including access to the unique mindset and skillset of a hacker. A former hacker can help not only in testing for vulnerabilities but also in responding to attacks. As one respondent put it, "Nothing beats a poacher turned gamekeeper." Indeed, more than a quarter of organizations (28%) have been using ex-hackers for more than two years, and another 28% have begun doing so in the past two years. Why? As another respondent explained, "Because they can think like hackers and know what they would do to prevent [one]."

The growing acceptance of hackers in the workforce is fueling an interesting phenomenon: hacking as a vehicle for professional advancement. While some hackers act solely with malicious intent, others commit the crimes as a means to an end. Seeking to build notoriety, they launch a headline-grabbing attack. They want to be caught—and acknowledged. After serving their time, they transform the crime into a "calling card" for a lucrative and legitimate position in information security. Of course, when interviewing any hacker, employers must weigh the risks and do their best to differentiate the career builders from the career criminals.

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.