VULNERABILITY MANAGEMENT

# CISOs: Do You Know the Security Risks of Your Organization's Next M&A?

Chris Evans

CISO and Chief Hacking Officer

(ghostwriter, Jenny Kanevsky)

June 14th, 2022

SHARE

In 2021, the global M&A market grew at a far greater pace than observers thought possible. According to McKinsey, large deals increased by 67%, peaking at $5.9 trillion with nearly 11,000 deals, rising 37% from 2020. M&As continue to grow this year, but certain factors make them more complex, including geopolitical issues, inflation, regulatory oversight, digital transformations, etc.

However, working with ethical hackers can make your M&As more secure and protect your organization from acquiring unwanted vulnerabilities and risks. HackerOne's recent acquisition experience, discussed below, is a perfect example of securing an M&A and minimizing inherited risk.

First, I will discuss the inherent risks of M&As as attack surfaces grow.

**A Growing and Unprotected Attack Surface**

An ever-expanding attack surface is a global concern for most organizations and complicates an M&A, especially for CISOs. The M&A prospect may have a partially unprotected attack surface, thus increasing security risk from a gap between the attack surface they can and do protect and the attack surface (and accompanying assets) they need to defend. This gap is what many M&A prospects bring to the table. While an M&A may have an undisputed business and strategic value, CISOs must still address the security risks involved in acquiring another organization's assets and its current attack surface, fully protected.

HackerOne recently released The 2022 Attack Resistance Report, where we surveyed 800+ company IT executives across American and European organizations. Our goal was to understand the impact of a rapidly changing application landscape on an organization's readiness to defend against cyberattacks. Overall, organizations reported only 63% of their entire attack surface is resistant to attack, leaving a vulnerability gap of 37%. That gap is significant, but on average, over 44% of those surveyed also stated they lack confidence in their ability to address the risks introduced by this gap. If your organization plans an M&A, you may acquire a 37% vulnerability gap, which equals security risk.

**M&A Diligence May Not Be Enough for CISOs**

For the CISO, evaluating security is a standard part of M&A diligence, but the outcome rarely changes the core "go/no-go" decision. Furthermore, diligence is often checklist-based, supplemented by automated tooling, or both. These methods may miss identifying the vulnerabilities and flaws in an organization's security, attack surface, and unprotected assets. When M&A closes, the CISO often does not accurately assess the new unit's security. In addition, the acquirer is immediately responsible for the risk of the new unit's assets.

**HackerOne's M&A Experience—How a Bug Bounty Eliminated Risk**

At HackerOne, we recently went through an M&A and are thrilled with the recent PullRequest acquisition. PullRequest code reviewers can accelerate engineers' development work by connecting them to instant expertise in secure code review.

PullRequest's technology builds on our history of improving application security and emphasizes developer-first solutions. PullRequest reviewers prevent bugs from reaching production by offering software testing closer to development. This helps our customers close their attack resistance gap between what they can and need to defend.

As HackerOne's CISO, I was immediately responsible for any business risk associated with the acquisition of PullRequest. Of course, I turned to our product portfolio to help address any possible risk. We quickly brought PullRequest into the scope of a bug bounty program using HackerOne Bounty.

We added PullRequest assets for the bug bounty, which notified all hackers subscribed to our program. We started seeing valid security vulnerabilities come in **within the first hour.** The immediate results continued. Within 48 hours, we had received 23 submissions, including a valid high-severity issue. The high-severity issue was a blind Cross-Site Scripting vulnerability disclosed here. This discovery—and the program's overall success—illustrate the power of the

ethical hacking community. This high-severity bug had been live in the product for five years. When our hackers were invited and incentivized to look, they found it within 21 hours.

Using HackerOne Bounty, we immediately addressed the security risk of our acquisition of PullRequest, undetected during diligence.

**Conclusion**

Rapid digital transformation, globalization, M&As, divestitures, restructuring, and more are just a few factors that contribute to the increased demands on security teams. Many are understaffed and lack training. Yet, it's difficult for many organizations to find the time and resources to address these issues. There has never been a greater need for hackers' immediacy, expertise, and creativity to supplement security teams and their current processes and automated tools.

The HackerOne Attack Surface Management Platform, now more robust with the recent acquisition of PullRequest, can help your organization eliminate M&A risk, protect an ever-expanding attack surface, and close your attack resistance gap. Contact us to learn more about achieving attack resistance with HackerOne.