Is Grey Hat Hacking Ethical

Redji H. Jean Baptiste

Algonquin College

CST8300

Rapid discovery closes dangerous holes sooner

Grey hat hacking is ethical because it leads to rapid discovery that closes dangerous and malicious holes sooner. The market that is a result of grey hat hacking has led to many discoveries in the field of information technology, with researchers uncovering critical vulnerabilities that would have remained hidden for months or years through traditional internal security audits alone. Both vendors and security researchers rely on this market to identify and patch vulnerabilities in software before malicious actors can exploit them for harmful purposes. In many cases the vendor would not have patched the software if the vulnerability was not made public, as companies often prioritize feature development and revenue over security maintenance and IT, when vulnerabilities remain hidden from public scrutiny. This can lead to an insecure security posture that could be exploited by advanced and targeted attacks from sophisticated threat actors who discover these same vulnerabilities through malicious reconnaissance. By having a grey hat hacking economy, it forces continuous improvement and development, leading to a more robust security posture across the entire technology ecosystem as competitive market forces rapid vulnerability discovery and responsible disclosure practices.

Erodes user and institutional trust

Once a vulnerability is made public, depending on the severity of the attack, it could lead to a loss of trust in the vendor or the institution to keep their and their customers' data secure. This issue is most prevalent in B2B and public sector contracts when a public institution relies on a vendor to provide software services for operations, as government agencies and large corporations have strict accountability requirements that make them highly sensitive to any perceived security weaknesses in their technology partners. Depending on how the vulnerability is discovered, the trust of that vendor to provide those services has been degraded, often resulting in contract cancellations, regulatory investigations, and long-term reputational damage that affects the vendor's ability to secure future

business relationships. The public nature of vulnerability disclosure creates a permanent record that competitors and critics can reference indefinitely, making it extremely difficult for organizations to rebuild their security reputation even after implementing comprehensive fixes and security improvements.

Real-life Example: Vastaamo Psychotherapy Data Breach (2020)

The Vastaamo attack demonstrates how cybersecurity failures completely destroy institutional trust in sectors handling sensitive personal information. Finland's largest private psychotherapy provider suffered a ransomware attack where criminals stole therapy session records of 33,000 patients, then individually extorted victims by threatening to publish their most private psychological details online. The breach triggered a complete collapse of public confidence in digital mental health services across Finland, with patient enrollment in online therapy platforms dropping dramatically as people lost faith in the security of digital healthcare systems. Vastaamo declared bankruptcy within months of the attack, and the incident sparked widespread questioning of Finland's entire digital healthcare framework, showing how a single security failure can undermine trust in an entire industry sector[1].

References

[1] J. C. Looi, S. Allison, T. Bastiampillai, P. A. Maguire, S. Kisely, S. Reutens, and R. C. Looi, "Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers," *Australasian Psychiatry*, vol. 33, no. 1, pp. 106-110, Feb. 2025, doi: 10.1177/10398562241291340.