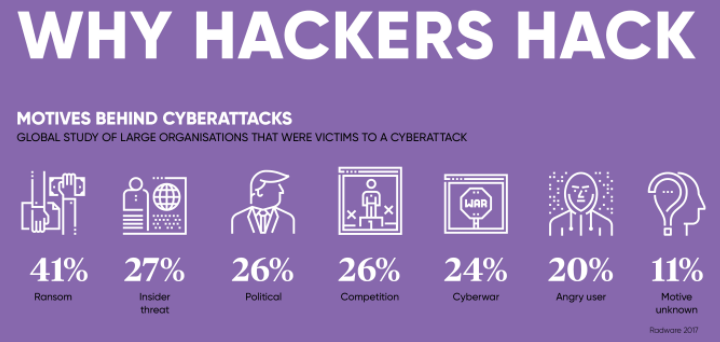
**7-1 Journal Consider the Motive for the Attack**

**Ryan DeBraal**

**CS-405-X6389 Secure Coding 21EW6**

I watched and read the resources provided for this module. I found them interesting and informative, especially the interview with Mike Loginov, who explained that many hackers do what they do simply out of curiosity and for accolades from their fellow hacker community. This surprised me as I assumed money would have been at the heart of most hacking incidents.

However, the infographics indicated that the motivations behind the actions of malicious actors is far more varied then I had at first suspected:



After reading the journal prompt, I’ve come to a somewhat unorthodox conclusion:

*Looking for the motivations behind a hack are almost entirely futile. It’s an academic exercise, something to be discussed in a classroom or in a book, but in the real world the point is moot.*

If I were explaining this to a new developer I would ask them: “Does it matter why a venomous snake would bite you?” The answer, at least in the short term, is an emphatic “No!”

Once bitten our priority *must* be to seek medical treatment. Down the road, when we aren’t dying of snake venom coursing through our veins (or in a business context when the corporation we work for isn’t hemorrhaging money due to the immediate fallout following a data breach) we can go back and examine the motivations of our attacker to our heart’s content. However, in both cases the reasons for doing so are most likely to answer the question: “How can we prevent this from happening again?”

Whether the answer is to wear longer socks while walking in tall grass or adding more layers of Defense in Depth (respectively), the motivation of an attacker doesn’t help us prevent the same thing from occurring again because hackers *hack* for a plethora of reasons including profit, political or religious ideologies, corporate espionage, good old fashion revenge or “just for the lulz”.

A threat can come from any direction and for any reason. Therefore, as a developer, we must try to be proactive by being imaginative. To me, the importance of reflecting on a hack is to better prepare ourselves for a future attack. In a zero-trust environment, we must assume everyone has bad intentions and develop our software accordingly; or to strain this metaphor nearly to its breaking point, we must assume that *all* tall grass contain coiled vipers ready to strike!

