Very few attacks happen just to be malicious intent. The amount of planning, patience and time that goes into an attack make it a serious endeavor. Every entity that gets attacked need to look at what they have to offer to an intruder. Personal PC’s have banking information and other personal data the intruder can use to either steal funds or use found data as ransom. Company’s have the same issue but also, they have political agendas that could be the focus of the hackers. I will apply this by thinking about what someone would want from when in regards to the code I am writing and use that as a starting off point to secure my data accordingly.

This might be a little difficult as new developers have a lot of skills but they haven’t been tested in the field as it were in a real-world scenario. They are hungry to get their hands dirty and start producing tangible results however I would sit them down and have an honest conversation about where we work, the services we provide and the likelihood of someone wanting to steal our data or hold us for ransom for one issue or another.

For an example I would use where I currently work. We are the largest exporter in the USA. The branch of the company I am in is the military services branch so we preform maintenance on many of the military aircraft platforms. A lot of state actors all over the world would love to get the data we have on the aircraft we have that the military uses. Also, we are building the new Airforce One’s. There is not a country on earth that would not like to know the inner working of the software on that aircraft. Understanding what is at stake behind the firewall is paramount.