The cyber security threats that individuals face are usually of the smaller scale but can still be considered dangerous and harmful. Whether it be to the person themselves (their location info, medical history, etc) or their possessions (bank account info, credit cards, key fobs) there’s quite a few risks that people should be aware of. For instance, some of the threats that you could face on a daily basis are things such as cyber scams around Black Friday and other holidays. Fake social media accounts can be used for phishing. Automated phone calls and text messages that try to convince you to open a link that will compromise your phone and the personal information that it contains. While these risks could be considered small when compared to that of which a large business might face, they’re still something to be wary of.

Small and medium businesses also need to be on the watch for phishing attempts as checking your email is a daily occurrence when working. Things such as mishandling sensitive information, such as a client, failing to use your mobile device securely, can allow unauthorized access to your organization’s network and files. A big thing that small and medium businesses need to ensure is that they have good password practices. Simply updating your password every 6 months by adding another number to the end of it isn’t going to cut it. Another major thing that companies need to be wary of is that their employees aren’t downloading any unauthorized applications. That fun looking “free game” to pass the time when you’re having a slow day, could easily turn out to be a malicious file that’s now compromised your network.

Large corporations, such as research laboratories and pharmaceuticals like we’ve seen recently, face a bigger and bigger risk to cyber crime every day. Once of the biggest threats they face is that of ransomware. A hacker will take their most important documents, client information, etc, encrypt it, lock it, and sell the key back to them. Which, unfortunately, most of the time, the business just pays for it. Malware, viruses, out-of-date software, social engineering (phishing, impersonation) and physical vulnerabilities (human error) are all risks that everyone faces but it’s definitely something that larger corporations will encounter more often than smaller ones.

By: *Curtis Crawford*