**Cybersecurity**

**What does it do?**

Cybersecurity is an umbrella term used for the variety of technologies aimed at ensuring the security of all types of computing systems in all areas at all times. It provides a level of protection between you and those with malicious intent. A few of the common categories within cybersecurity are:

* Network Security
* Application Security
* Information Security
* Operational security
* Disaster Recovery and Business Continuity
* End-User Education

Since its inception, cybersecurity has been a constant game of cat and mouse with the continuous power struggle between the IT industry are large and nefarious actors. The birth of Cybersecurity was in 1971 with the story of the “Creeper” and the “Reaper”. The Creeper was the original computer virus created by Bob Thomas. He created the program to propagate itself through networks and once a system was infected the computer would have a text document appear that says “I’m the Creeper: catch me if you can”.

The program wasn’t malicious and was a proof of concept for a theory from the 1940’s, which hypothesised that self-replicating programs were potentially possible. In response to the Creeper the Reaper was born, the reaper was the first form of an antivirus. The Reaper would disseminate itself across the network in a similar way to the Creeper, searching for any sign of the virus. When the Reaper found the Creeper, it would delete it to stop it from spreading further across a network.

Cybersecurity has rapidly evolved from these humble beginnings into the cutting edge technology it is today out of necessity. Today the cyber threats are far more complex, the world isn’t so black and white anymore and includes nation state actors that horde zero day exploits that have been deployed again friendly nations (e.g Operation Socialist: UK’s GCHQ infiltrated the Belgacom, Belgium’s national telecom using a technique called Quantum insertion) or spying on citizens .