Article

Jul 2021

The Telescoping Nature of Cyber Security

Understanding the exponential growth within Cyber Security.

Humans are great at solving immediate problems. For example, if someone were to throw something at you, you'd attempt to dodge it, right? But what if the threat wasn't so immediate? Say it's something simple, like avoiding extensive trips to the dentist. Although one thing we recognise is that it's clearly beneficial to floss and brush twice daily, still some people struggle. And I'm sure you can see where I'm going with this. Often at times, cyber security is a lot like that problem we ignore until we no longer can. The issue is: this problem was always present, but not particularly imminent. For example, less than a decade ago, particularly damaging techniques such as Ransomware had yet to be conceived, most software was fairly new and as a result didn't have multiple vulnerable versions and the dark markets and infrastructure to purchase or acquire leaked usernames or passwords did not exist.

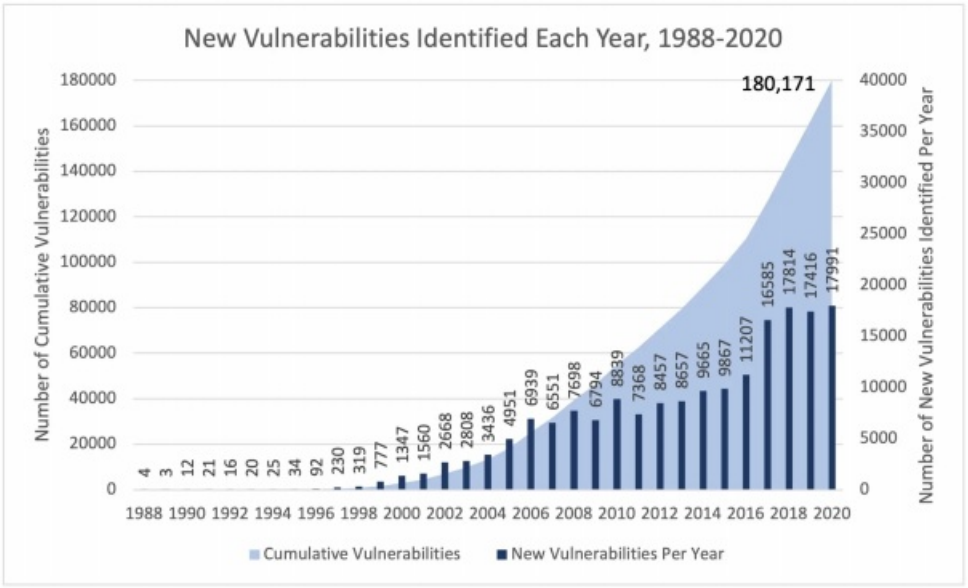
With time and deeper business IT integration however, we have seen a paradigm shift in the types of attacks that had previously been carried out. In the past, phishing, spam and in some cases, corporate espionage were the largest threats facing businesses, however with this growth of IT, we've seen businesses increase their online presence both internally and externally and in turn we have seen the growth and development of threat actors, their abilities and their techniques.

It's becoming more pronounced too, with headlines and disclosures of businesses that were previously thought mature, we're seeing cyber security root itself deeply in the common consciousness. As businesses increase their services and exposure, so too is there observable growth in external attackers abilities and techniques.

Earlier this year, market analyst firm, Canalys released a report detailing this change:

Although some of this may be attributed to the change to the 2019 amendments to the Notifiable Data Breach scheme of 1988, there's also been large changes in the way attackers have been conducting themselves. For example, in recent years, we've seen the rise of Ransomware As A Service (RaaS), in which malicious actors can, for a monthly subscription, purchase access to a ransomware platform to help manage and attack their victims. Again, year on year we're seeing an exponential uptick of estimated ransomware revenues with security firm, Fireeye estimating revenues from 2019 of 11.5 billion USD to 2020 which saw 20 billion USD.

However this is an example of one type of opportunistic attack, how about other threats? For a long time I've strongly advocated that your exposed services are only secure until a vulnerability is discovered. And they ARE being discovered. En masse:



Above is a graph produced by IBM's Security Intelligence detailing the count of all public vulnerabilities for software found between 1988 and 2020. Again, we're confronted with an almost bell curve culminating 180,171 publicly known ways to attack various software and services. With more developers, more software, more versions, more platforms, more hardware, more bug bounties, more hackers and more threat actors it starts to become abundantly clear this problem stands only to increase.

Similarly, the IT Manager's role has increased in both breadth and depth and so too has the role of the Security Manager and internal SOC. With more threats, more users and a growing IT surface to secure, it begins to make sense to share the load with a highly technical team. Myself and the team at Waterstons aim to provide exactly this. A managed security approach with respect to your business strategy, goals and assistance where needed; be it baselining your environment to protect against common threats, 24 hour in house monitoring and investigation of security events or helping your organisation meet its compliance goals. At Waterstons, we draw from almost 3 decades of collaboration and innovation to provide quality services globally, from our offices in both the UK and Australia.

If you'd like to learn more about our offering or have a chat about what we could do to help secure your organisation, please don't hesitate to contact our Cyber Resilience specialists or or email cyber@waterstons.com.