# WHAT POWERFUL LESSONS CAN WE LEARN FROM NATURAL DISASTERS?

On 14th March 2020 an article appeared in the Guardian, that World health organization has declared the CORONA VIRUS a PANDEMIC. The WHO has stressed that using the word "pandemic" does not signal a change in its advice. It is still urging countries to "detect, test, treat, isolate, trace and mobilize their people".

I am not a qualified medical practitioner, nor do I intent to be one. My interest lies in analyzing this from Cybersecurity perspective and key learnings for Information Technology sector.

The words ""detect, test, treat, isolate, trace and mobilize their people", resonated with a discussion I was having with a client a few weeks back

Cybersecurity has the propensity to borrow words from other fields. Words like Virus, Zero Day Attacks, Advanced Persistent Threat, insider threat, firewall, phishing, ransomware are some words that cross my mind which has a deep relevance to this article.

The epicenter or ZERO Day (this is still being debated) from where the virus first originated has now started reporting less cases. However, the cases in other parts of the world has seen a dramatic rise. This is where, we as cybersecurity professionals need to co-relate this to our field of business as enunciated below

1) Threat Intelligence: - Threat Intelligence has become an inseparable part of any Cyber-conscious organization which needs to stay ahead of the curve. This helps organizations to be PREDECTIVE and take proactive steps to tackle threats which can impact their business operations. The rumblings in the DARK WEB area are a stark reminder to organizations what they need to expect and be ready to mitigate or neutralize threats, thus reducing the RESIDUAL risks
2) Perimeter Centric Controls: The castle doctrine for cybersecurity strategies were used extensively to protect the organization in the good old days when we had all data concentrated in a data center with Cloud and BYOD concepts still in their infancy. Example of these controls could be firewalls, web application firewalls, IPS, NAC, EMAIL security etc.
3) Data Centric Controls: The adoption of Cloud and BYOD ushered in the "Perimeter no longer exists, and Data is everywhere "concept. Organizations started scrambling for controls concentrated around protecting data. Example of these controls could be DLP, Encryption, Data classification, SIEM etc.

4) Identity or user centric Controls: The last three to four years has seen controls mushrooming around securing identities or controlling user behaviour. Example of these controls could be SSO, Multifactor authentication, UEBA, PAM etc.
5) Conjoint Controls: Last few years a new school of thought " INSIDER THREAT " has taken root , with organizations deploying conjoint controls – a combination of user/identity and data centric controls

**So how does this all relate to the Corona Virus outbreak?.**

Perimeter based controls relate to the external blockade imposed by many countries including ban /cancellation of flights, screening of patients at airports, travel bans, visa bans, quarantine facilities at airports (akin to sandboxing techniques). This has definitely helped restrict new cases at the borders

The sudden spurt of cases in many countries many months after the initial outbreak points to the dormant nature of the virus and how it has managed to pass the perimeter-based controls. This is where the Defense-in-Depth approach plays a vital role. Governance tools, Business continuity and Disaster recovery plans need to be operationalized, with deployment of conjoint controls that target both data and the identity/user. Closure of schools, malls, lockdown of cities are all measures which help reduce /mitigate insider risks.

However RESIDUAL risks still exist, and AWARENESS then becomes key coupled with THREAT Intelligence to disseminate correct and right information. We the people are the WEAKEST LINK. Risk aware individuals armed with the right INFORMATION, can lead to RISKs being ELIMINATED.

This article in not an attempt to discredit, find faults or criticize any individual, organization, country or government. However, as a responsible citizen of this world and a concerned human being, it is but natural that we learn life lessons from natural disasters. Interdependence of Information technology on every aspect of society can help us build the strength and resiliency into our lives.

Reference : https://www.theguardian.com/world/2020/mar/14/what-is-a-pandemic-coronavirus-covid-19

Roshan Neville Sequeira

Email – roshan@secureworkspace.tech

M- +971 5444 27566