Principles of Security and Human Sickness – A Correlation

Sure, readers may be intrigued with the title of this article; however, this article is a result of real-life experience. This incident involved my son; it happened in December 2018; when we were attending the midnight Christmas service in the church. This article is retrospection on the unfolding of events of that week.

Part 1

Halfway through the service, my son complains of giddiness; our first reaction is to seat him; give him water and ask him to relax. Just like any concerned parents; we dig into our experience and quickly conclude; it is late at night, and he needs rest. We continue with the service; our religious obligations and beliefs over-riding our fears

Introspection

1. Did we as parents have enough empirical data to back out first response – offering water OR we believed in what we had heard, read, or observed.
2. Was our response DEPENDABLE? Is water the first line of treatment for giddiness
    a. Are the Threat Intelligence programs deployed in our SOC Dependable; Do they have Empirical data to make informed decisions?
3. Do employees of an organization, security teams, SOC, Senior leaders react to an incident in an analogous manner; drawing on our experience; offering automatic reactions, our priorities over-riding our obligations towards compliance and more in-depth investigations?
4. Did our response to the incident help meet the desired goals- tactical and strategic? was our son's health issue resolved
    a. Security organizations react comparably to client's needs. We fail to understand their business objectives or their needs
    b. Organization's offer client products on their approved list, based on skill sets available, drawing on previous experience and knowledge of their product capability
5. Is this how reconnaissance by hackers overlooked leading to severe breaches?

Part 2

As time elapses; the symptoms persist. We rush our son to the church clinic, staffed by a couple of nurses. They follow the Standard Operating Procedures – Check vital parameters, ask questions, make my son lie down, and check him. On completion of the SOP; they announce that things are okay with a warning; a second opinion by a specialist can help rule out all possibilities.

Introspection

1) Was the Nurse Efficient and Effective?
    a. She was EFFICIENT in her work; based on her training and standard operating procedures she performed her duties to perfection
    b. BUT she was not EFFECTIVE; trained as a first responder; however, she lacked the qualifications and skills to treat my son (She was neither a qualified physician nor a specialist)
    c. The place was a clinic and not a full-fledged hospital.
2) Are clients not misled by Security organizations who claim to be specialists; while they are just nurses?
3) There is a fundamental difference between Awareness, Training and Education. Training helps acquire the skills for a specific role – SOC Analyst, for example.

4) Security has trade-offs – Time, Money, Resources, personal preferences, history. Organizations are enmeshed in trade-offs leading to sub-standard services – Efficient but not Effective.
5) Organizations need to be visiting specialized hospitals replete with qualified and trained specialists and state of the art equipment; they end up at clinics
6) Managed services are gaining in popularity – managed SOC, Managed SIEM. Managed SOAR, to name a few – It is imperative not to fall prey to propaganda and marketing, but make wise choices

Part 3

We visit a specialty hospital the next day; armed with an appointment with the pediatric. She recommends a series to tests related to her specialty - a point to remember here- (the labs are in the same building; so there is minimal delay and reports are made available on priority- as an in-house Dr recommended us)
As the tests are negative, the diagnosis is inconclusive; and ENT and Neurologist conduct additional tests to rule out all possibilities. The results are available on priority, all tests are in-house, and the diagnosis is complete. All this happens in a single visit, saving considerable time, money, and efforts.

Introspection

1) My SON is my asset, and I was able to accord his health highest priority
    a. Organizations need to discover their assets, categorize them, and classify them based on business objectives
    b. Management base their decisions on Risk Analysis of these assets – It enables management to allocate the right resources for their protection and upkeep.
2) Centralized record-keeping helped in better identity and access management.
    a. It was like a Single Sign-on solution, identified and authenticated only once on arrival.
3) Having multiple specialists under one roof helped in faster diagnosis, better consultation, and speedy resolution.
    a. Imagine if I would have to visit a different hospital for different specialties; explain the situation to each one of them- It would cost extra days, and the effect of this delay on my son's health could be anybody's guess.
    b. One of the principal objectives of GOVERNANCE is Optimization of resources- Time, People, Processes, Data
4) The Pediatric built a baseline of my son's health condition, the ENT and Neurologist built upon it to arrive at faster resolutions.
    a. The Pediatric briefed the ENT, who had his job cut-out; similar was the case with the Neurologist –reported by the ENT, the expectations were clear.
    b. For organizations to understand their security posture, it is imperative to measure it against a baseline; however, they need specialists like the Pediatric, ENT, Neurologist with a wealth of experience, complete with industry and domain knowledge to assist and recommend in the right areas.
    c. Various departments need to work in harmony and have access to standard DATA and Knowledge to allow management to make informed decisions
    d. Communication is KEY, and uniformed output is fundamental to prevent errors in judgment
5) Different tests under one roof helped me save time, money, and efforts of visiting various lab facilities
    a. Inconclusive results from different tests did not hinder in the progress; it helped build on it and arrive at a conclusion. Security is not about a single product "One solution fits all.",

The attack surface is vast, the threat actors spread far and wide; a plethora of different solutions and technologies coupled with human intelligence is the need of the hour.

b. Governance aims to remove Silos from within an organization; better coordination, faster response, and resolution; not to mention better customer satisfaction, thus bringing in the much-needed loyal customer base.
c. In many organizations, the Security team evaluates a technology, or a solution based on strict technical parameters; however, the procurement team determines their purchase solely based on prices.

6) Road Map- The pediatric acting as a trusted advisor provided a roadmap; the Do's and Don'ts's, how to better care for my son, the root-cause of his sickness and the path to recovery.
    a. Security has evolved; organizations need a trusted advisor to guide them on the journey, with a thorough understanding of the business needs and the changing landscape.
7) Certified and regulated by various bodies, the hospital met all obligations laid down by LAW, was compliant to different health standards, and audited by external auditors.
    a. These certifications and accreditations by reputed external bodies provide me with an assurance of better management of risks - Examples below:
        i. Least-privilege – Only Doctors had access to my son's records. No hard copies of patient files circulated from one Dr to another.
        ii. Need-to-know – The different labs and test facilities could only access records about their labs. The ENT Labs could not access documents of the pediatric tests.
        iii. Digitization of records and Centralized repository: Each Dr could access the patient record from a centralized repository; view the complete patient history, make informed decisions while prescribing medications

Hospitals are not brick and mortar building, and it takes years of painstaking challenging work to achieve a reputation and the confidence of their patients. What differentiates a hospital with its amalgamation of specialists doctors, their wealth of experience, the specialized equipment's and support staff is "ONE STOP SOLUTION FOR A PATIENTS NEEDS".
A run of the mill security organizations with mediocre facilities and skills are best suited for tasks like the clinics. We cannot expect them to invest in research, to offer specialized expertise in multiple areas of security technologies and products; while providing a comprehensive ECO-System of solutions; integrated to the tee. It takes years of painstaking labor to get certified against industry standards; the efforts increase manifold to maintain them.

The reader might find my introspection points mundane; old wine in a new bottle, or even perhaps capitalizing on my son's sickness. The moot point I want to drive here is Simple" You throw peanuts, you get Monkeys."
Security is not rocket science, yet security is also not marketing and products. Security is a journey; new products, new specialties, new technologies; we need to offload the old and embrace the new- Security Organizations who become our fellow travelers on this journey need the right compensation; least you end up with monkeys.
"It takes TWO to TANGO – The organization who needs security and a responsible, reputed, reliable, trustworthy organization who can provide for."

Roshan Neville Sequeira
Email: roshan@secureworkspace.tech
Mobile – +971 5444 27 566