Security is Everybody's business

Security is Everybody's business, is a cliché which reverberates in every forum, advertisement, discussion, conference and organization. However, very little gets done to dispel the myths and obscurity surrounding information security- its use, applications and its study.
It is upon security professionals to pool in our collective knowledge and help ease the pain and burden; so often felt by the uninitiated; that Information security is no rocket science, but simple tasks we do in our everyday life. This article is an effort in this direction.

Part 1 lists five scenarios and questions; Part 2 explains how these five scenarios relate to information security.

PART 1
Scenario 1.

Seated on the driver's seat, hands on the steering, foot on the gas pedal, you look up the dashboard. The fuel needle indicates the tank is full, gear is in DRIVE state, the temperature is average, and tyre pressure is within the range.
Next, you look through the windshield and windows – every one of them is blackened, offering no view of the outside world.

A few questions for the reader

1) Can you drive; move the car forward, backward or sideways?
2) Would you risk your life, and those you are responsible for, without a change in the situation?
3) What advantages does a clear windshield and windows provide to the driver?
4) Is the driver better positioned to make informed decisions concerning the dangers, thus mitigating the chances of an adverse incident?
5) Can the driver use the controls (Steering, gas pedal, gears) more effectively and efficiently?

Scenario 2-

COVID-19 is considered life-threatening to patients with co-morbidities; these fall under the "high risk" category. When the virus infects an individual with co-morbidities, a team comprising specialists from various fields team up to treat the patient.

A few questions for the reader

1) Why does one need a team of specialists to treat a common virus; Can't we have a doctor who has all the required expertise to manage all medical conditions?
2) Would it be possible to have a small clinic or mediocre healthcare facility assemble such a team?
3) How does it impact the response to treatment, knowing the level of care and attention required?
4) How is a large hospital able to attract top talent as compared to a small clinic or healthcare facility?
5) What helps the hospital retain talent – better exposure to latest global knowledge, advanced equipment's, membership access to extensive global medical bodies or forum, etc.?

Scenario 3

You visit a general practitioner/physician with a symptom of common cold, headache and fever. The prognosis (an opinion, based on medical experience, of the likely course of a medical condition) suggests your body is fighting an infection or illness caused by a virus, bacteria, fungi or parasites; common in both adults and children. In some cases, they may signal that your body is fighting a more severe infection or illness

The general practitioner/physician generally advises a line of treatment for seven days. Persistence or worsening of symptoms leads to two scenarios

a) Refer the patient to a specialist
b) Conduct a few medical tests (example- blood tests).

Further on, if the tests are inconclusive, more advanced tests like MRI, CT-scan, etc. could be ordered.

A few questions for the reader

1) Why can't one test provide all the illness plaguing the human body; furthermore, what additional information is available from advanced tests like MRI?
2) Why would there be a need to be referred to a specialist?
3) Is the Physician not experienced enough to treat the disease?
4) Does this hurt your financials, strain your resources – time, energy, efforts.

Scenario 4

As you walk the park with your spouse, you stumble and fall. Your hand hurts terribly, and bruises appear on the knee. You get up, brush yourself, apply an antiseptic on reaching home, and life goes on.

However, while walking the park if your spouse were to have a cardiac arrest, it would be best if you act fast, call the ambulance and also try to provide CPR.

A few questions for the reader

1) Are you trained to provide CPR; are you prepared to react to an emergency; Do you have experience in dealing with such situations earlier?
2) Is an individual required to be trained and educated to respond to every situation in life?; Why do we fall back on trained professionals; individuals with specialized skills.
3) Why did the first incident not solicit the same response as the second incident?
4) Can Drugs like the Antiseptic (available over the counter) act as "One medicine fits all "remedy?
5) Why does the cardiac arrest call for a completely different response as compared to the "fall in the park."

Scenario 5

It's time to buy a new television for the home. The family members huddle together and brainstorm- Brand, features, dimensions, Technology, price, place to buy etc.
Contrast this with buying furniture – The discussion would revolve around the type of wood, single or double bed, type of mattress, placement in the home etc.

A few questions for the reader

1) Would the stakeholders be the same in both the above scenarios?
2) A Television caters to the entire household as compared to the bed, which might be more individualistic.
3) Is Brand a more significant consideration for the bed as compared to the television
4) Are issues like after-sales service, updates, upgrades, life span more critical to the television vis a vis the BED?

PART 2

Scenario 1 - Why is "Visibility" a critical factor in Information Security?

Visibility into the security posture of an organization helps the board or management (responsible for the organization, its assets, people, process and data) make informed decisions. It supplies critical information on the effectiveness and efficiency of the controls deployed and effectively mitigates risks.

Visibility enables an organization to understand the current "CONTEXT". The online Merriam-Webster dictionary defines the meaning of context as - the interrelated conditions in which something exists or occurs: environment, setting.
Thus "Visibility" aids and assists an organization to - make informed coordinated decisions, prioritize actions, Minimize risk, Be better prepared for the unknown, Plug loopholes amongst many other things.
The steering wheel, gas pedal, gears are mere controls; ineffective and in-efficient in the absence of visibility.

Scenario 2 - Why does an organization need different technologies to gain visibility?

Specialists in a hospital are akin to the different technologies deployed by an organization. It is imperative to gain a 360 view of the happenings with the organization. Just as the field of medicine has advanced over time with new specialities, so has the area of Information Security. With the world moving towards an application-based economy, the traditional boundaries governing the world of information security has disappeared. The proliferation of the internet, mobile devices, cloud services and internet of things IoT has made organizational resources spread thin; causing immense hardships and misery.

An organization at the very least needs to have deployed an NDR, EDR, SIEM+ UEBA solution if it needs to stay abreast with the latest happenings inside their organization. However, the CRUX of the matter is not to deploy the technologies mentioned above but to ensure that they work in harmony with the larger eco-system.
An ad-hoc approach makes organizations end up with multiple technologies; each on their own; unable to provide a consolidated view. *Bill Gates once said, and I quote "Technology is just a tool. In terms of getting the kids working together and motivating them, the teacher is the most important."*

Scenario 3 - Why does an organization need specialized skills in various technologies?

The old-age adage "One Size Fits All", needs to be consigned to history.

An organization comprises of four crucial pillars – People, Process, Technology and Data; People access the Data through Technology using a Process.
Security vendors inundate organizations with offerings espousing cutting edge technologies laced with marketing jargons; Machine Learning, Artificial Intelligence, Cognitive learning, to name a few.

Many organizations claim to employ individuals with a wealth of industry experience and knowledge; however, there is a significant difference between Security Wisdom and Security Knowledge.
Wisdom is a combination of industry experience coupled with in-depth knowledge of a specific subject or domain.
Organizations must hedge their bets on a service provider with a deep-rooted history of innovative offerings; industry leaders replete with R & D facilities.

Scenario 4 – Why are Training and Specialized skills an essential hallmark of information security

" Jack of all trades, Master of none" is well known saying. However, it does not apply to specialized fields like medicine and information security.
Would you trust a doctor with your life, if not for their qualifications and experience? Confidence in the doctor and his reliability to treat a particular disease; is the beginning of a robust doctor-patient relationship.

Organizations need to engage in activities they do best; leaving the specialized tasks of information security to organizations which excel in this field. A car manufacturer is best suited to provide its clients with competitive cars; leaving the skilled job of information security to an organization which does it best.

COVID-19 has been an eye-opener; organizations were over-night shifting to a new way of working from home. Those with in-house staff or lacking contracts with third-party service providers faltered; unlike organizations with contracts with specialized vendors.
Global specialized vendors with their client experiences across the globe; build best practices quickly; offering cost-effective solutions. Remember, COVID-19 hit the world in December 2019, but the countries which went into lock-down differed across various continents.

Scenario 5 – Security Tradeoff's

Like every other field, information security is not bereft of trade-offs. The line between "Good to Have "and "Must Have" is continuously blurring.

Crucial decisions related to service- tactical and strategic; business continuity; incident response take a backseat; departments or business functions spar over one-upmanship, leading to purchases which either do not meet the business objectives or fulfil them partially.

Conclusion

We must understand that our work in information security is no different from what we experience and expect in our daily life. When we co-relate happenings in our lives with decisions related to information security, it might result in seeing things in a different light.

Decisions we make in our everyday lives are risk-based, strategically sound, tactically enforceable; replicating them at our workplace might help ensure the same results.

Regards,

Roshan Neville Sequeira

Mobile – +971-54- 4427566

Email- roshan@secureworkspace.tech