Protecting Secrecy vs Increasing KPI: Cybersecurity Perspective

TECH By **Sabbir Hossain**

October 13, 2021

This pandemic era has rehabilitated us in many ways. From our daily routine to buying habits, from our learnings to our professional life. Only common thing in all these habits is undoubtedly “connectivity”, more precisely, internet. Even before the pandemic you can find some people comfortable in doing errands physically than online like shopping or banking are transformed in this era. With this growing transformation in habits, cybersecurity is not a luxury anymore rather its one of the very primary requirements for every business as well as for every individual. To keep up with these growing requirements we see growing competitions as well as large numbers of cybersecurity businesses who are trying to fill-up the gap. There are new service providers and many of them have simply converted to cybersecurity business from IT or even non-IT business backgrounds. Here’s the problem starts. From ages we have seen a competition among businesses who sell similar products. We have seen advertisement-counter advertisement and counter-counter advertisements of Pepsi &Coca Cola in recent pasts. There are numerous direct and indirect competitions in retail industries and this competition sometime actually is beneficial for end users!

But the scenario is completely different in cybersecurity. If we say what is the very primary objective to purchase security products and services from customers perspective, we can summarize like: “Protect Business and Customer Data, ensure availability of business online and ensure the integrity of data”. That’s basically the concept of CIA triad which is the very basic of cybersecurity. If we imagine the products and services offered by cybersecurity vendors, its always something that deals with very confidential data of either the business or its clients. For example, if we are talking about a firewall or IPS/IDS, we have several confidential information

in hand. We have attack vectors, attack occurrence timestamps, infected machines details and so on and so forth. If we are talking about services like VAPT, the scenario gets even complicated. The pen tester then has piles of confidential information including the exact holes of the systema and architecture and future attack soft spots. Here comes the business perspectives. In name of competition or simply increase KPI the service providers often disclose confidential information of one client to another.

I want to share a few real-world examples I faced in past few months. First, few days back I was in a webinar where one representative of a vendor shared a case study from a client premise and at end of his presentation, he mentioned that as that client has manpower crisis, the problem is still wide open unresolved.

The second incident was in marketing material of one of the service providers who shared list of issues of a few clients and claimed all have been resolved using their solution. In the material there were a few points which can point a direct finger to the capability of the client and can insist perpetrators to try and break into their system again.

The third scenario is pretty common. We often see responsible personnel from service providers disclose every bit and piece of the incident to media and press. Which do not bring anything good for the investigation or future. One classic example is, when a central bank heist happened, someone responsible disclosed in media that there is 10$ routers used across banks resulting few more attempted hackings in banking networks.

All these three incidents are examples of irresponsible disclosure of clients' information. For service providers its very common to share inside details of one client to other to earn the trust and workorder. The main reason behind this is the competitive mindset. We probably are not looking "Cybersecurity" business as "Security" business. Can anyone tell me how many interceptions system is there in a country? Or how many Missiles or radar or Anti-aircraft system? This information is marked as "Classified" and protected in such a way that's beyond public eye. This tradition is there for years and all the vendors and service providers are used to this custom for long. We need to initiate same practice for cybersecurity as well and strictly protect interest of client and customers details. Often just to boost the KPI, individuals are sharing confidential information to other clients, to media or even to public. This practice must be finished.

We need to understand that data is the new gold and we need to protect those at any cost. Data protection acts are protecting currently many parts of it but its not helping much to change human behavior of sales and marketing teams or even to management who feel proud bragging about their works. We need to make sure what exactly we can share and to whom. Clear traffic light protocols should be implemented along with active practice of it. Every member of a team should be trained to protect secrets and keep privacy of the clients. Every cybersecurity

practitioner must come forward and ensure the secrecy of information. Together we can make cyberspace a better place.

Author Recent Posts

Sabbir Hossain

A cybersecurity practitioner with 10+ years of experience in both technical and management domains. Have experience in intelligence and forensics equipment's like lawful interception or data extraction at first part of career for 5+ years. The second part of my career was managing national as well as multinational teams of highly technical personnel and lead them from the front for both for Government and MNC. Served as local technical support person, IT security consultant, Managing director for a multinational company's local entity as well as chief coordinator for Bangladesh Government Critical Infrastructure IT Audit & Risk Assessment team. Vastly experience in Middle Management & Senior Management. Participated actively in preparation of several policies and act which were later adopted by the Government of Bangladesh.

Currently enrolled in University of Ottawa. Received IBM research fellowship and working on Cyber Crime Domain.