CYBER THREAT INTELLIGENCE -

A PARTNER IN RISK MANAGEMENT

MUNEEB IMRAN SHAIKH

CISSP CRISC CCSP PMI-ACP

https://www.linkedin.com/in/muneebimranshaikh/

RISK MANAGEMENT - A LYNCHPIN

In this world, what distinguishes individuals, societies or organizations from each other is their capacity to plan, address challenges and seek opportunities to grow and create a value in the society.

Risk Management is a discipline that enables the individuals, societies and organizations to address the challenges they are facing or are likely to face in achieving their mission, helping them pursue opportunities for growth and value creation.

Risk Management is a reflection of maturity, a demonstration of due care & due diligence contrary to the notion of blindly accepting challenges, moving from one crisis to another and considering it "Resilience." However that being said, it takes a substantial time and effort to have an effective Risk Management program established in an organization to deliver its objectives.

PERCEPTIONS OF RISK

As organizations embark on the journey to set up a risk management program, they are immediately encountered by a challenge of perceptions associated with risk scenarios. This challenge is not limited to the realm of Information Security but spans across broader policy frameworks, constrained not only within the organizations but also within the government sectors where broad based policies are formulated.

A recent example of varying perceptions of risk has been seen during the COVID- 19 Pandemic among the health specialists and policy makers between adopting a policy of stern lock-downs to prevent the health systems from collapsing while the other section has cautioned against stern lock-down which could give birth to many other issues including hunger and poverty.

It is fair to say that teams and organizations often overestimate and underestimate risk scenarios leading to incorrect estimation of impact and misperception of Risk subsequently leading to disastrous consequences. This makes the entire Risk Management function a Vulnerability in itself.

These varying perceptions of Risk often inflict tendencies among Information Security Risk Professionals to apply a multitude of controls to establish and maintain a Secure Posture. It is worthy to remember that security controls create friction and affect the business velocity and pace. Business exists to achieve their goals, mission and objectives and not for the sake of establishing a stern secure posture. Security Controls are therefore supposed to be implemented to facilitate the organization in achieving their goals, mission and objectives in a secure manner and maintain that equilibrium for sustainable growth and value creation.

So how do organizations deal with the misperceptions associated to risk to ensure correct estimation of Impact? One of the significant factors that determines risk is Threat. If there are vulnerabilities within the environment but no associated threat then the risk does not materialize.

As Organizations engage in Risk Assessment exercises, it is availability of data that becomes a primary factor to decide whether a Qualitative, Quantitative or a Semi-Quantitative analysis approach will be adopted. Threat-centric risk scenarios are derived from examination of Threat agents and the vulnerabilities exploited by Cyber Criminal or other Threat Actors.

Adopting a Threat Centric approach keeps the Risk Management team abreast of potential methods of attack, threat actors and cyber criminals targeting the Industry vertical or region along with their motivations.

WHERE DOES CYBER THREAT INTELLIGENCE FIT IN ?

A Cyber Threat Intelligence Team liberates the organization's Risk Management function from misperceptions by providing the actionable intelligence which can be used to select or design associated controls. However organizations need to first understand various drivers and trends associated to threats in order to accurately subscribe to and consume Cyber Threat Intelligence.

It is unfortunate that Cyber Threat Intelligence has become a buzzword and its implementation is often limited to the consumption of Threat data feeds which are often volatile and tactical in nature and therefore do not add value to the Strategic objectives of the Organization.

However I must not digress to discuss the details of effective Cyber Threat Intelligence Function and the kinds of Threat Intelligence, an organization should subscribe to.

With Strategic intelligence readily available, an organization becomes equipped to better protect their Organizational assets and enable themselves to achieve the goals or mission set out by the Senior Executive Management.

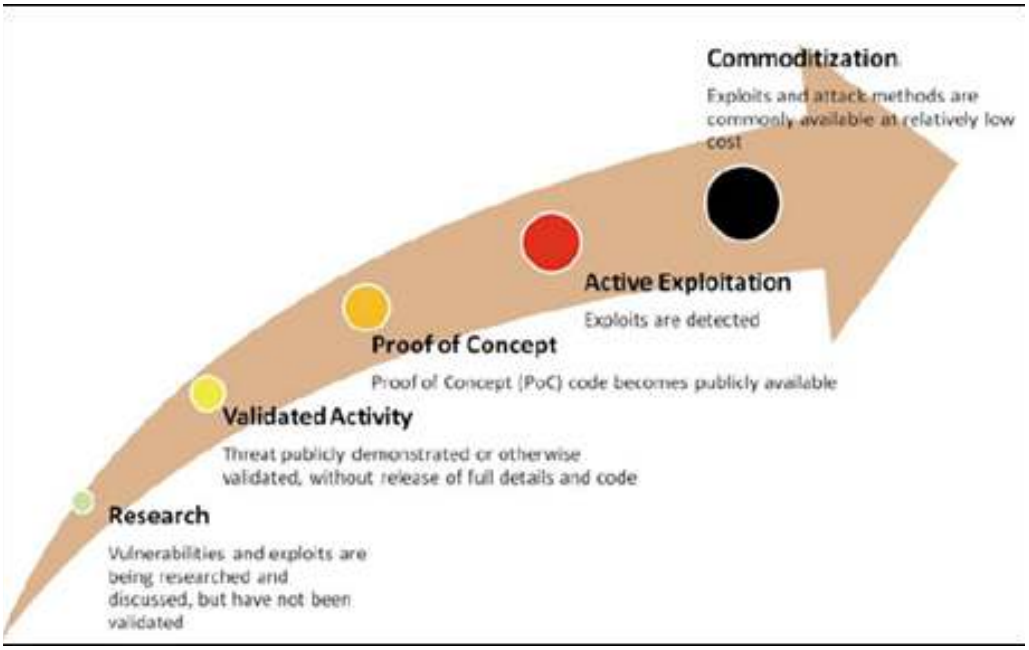
The Information Security Risk professionals need to have following reliable information while creating and assessing of risk scenarios:

- ***Current Trends & Drivers likely to affect the Business in short & long term.***
- ***Threat Actors targeting the Industry or Region.***
- ***Number of times certain attacks have been observed by other enterprises in similar Industry.***
- ***Nature, Pattern & Methods of Threats and Attacks.***
- ***Are the vulnerabilities exploited by Threat Actors present in Enterprise?***

INCORPORATING PRODUCT LIFE CYCLE MODEL

Intel Corporation presented a Product Life cycle model for tracking the evolution of threats. The model recognizes that many threats emerge as theoretical risks but progressively mature as their exploitability is demonstrated, their proof of concepts become publicly available and eventually their products are commoditized.

This model helps to communicate actionable information to Risk Committees or Security groups to determine when and where to allocate resources to deal with identified threat based on its maturity and likelihood to affect enterprise.



Source Intel Corporation, 2012: Product Life Cycle Model - Tracking Evolution of Threats.

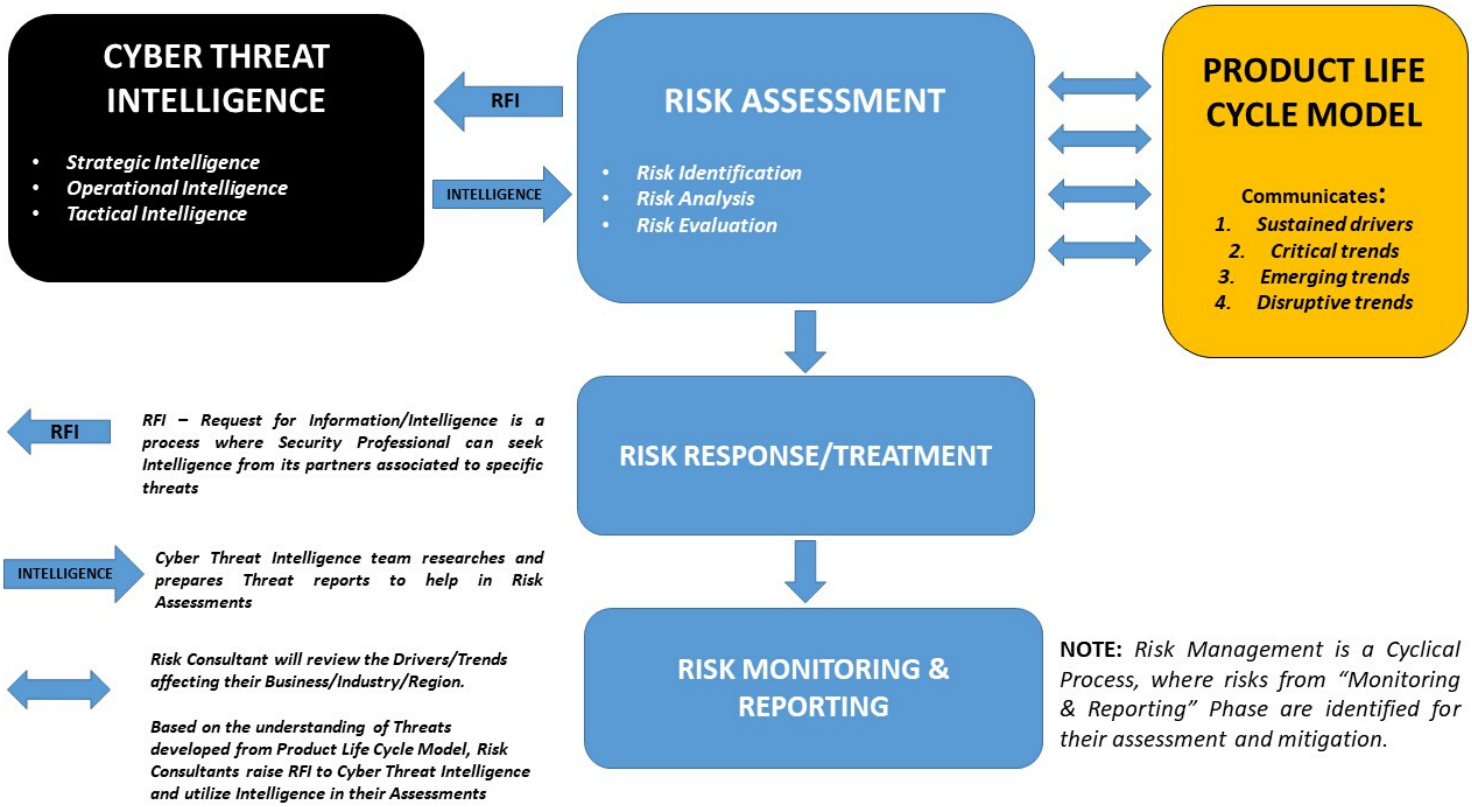
The product life cycle model groups the activity areas into four main clusters, depending on their *level of activity, maturity potential* and on their *potential impact to the company*.

Trends/Drivers	Description	Examples
Sustained drivers	Areas that already have a high impact or otherwise cause considerable concern.	Malware and Web attacks.
Critical trends	Areas that have begun undergoing active exploitation, with growing adoption beginning to shift toward commoditization.	Social computing & Smartphones
Emerging trends	Areas that have a low current level of exploitation, but considerable research and proof-of-concept activity	Embedded & Cloud Computing
Disruptive trends 	Areas with little or no active exploitation, but significant research activity and the disruptive Potential to cause a major security problem. Frequently, they are discussed as theoretical risks, and because of this, many people in the industry would be caught off guard by a significant event.	Virtualization

Source Intel Corporation, 2012: Product Life Cycle Model - Tracking Evolution of Threats.

By Incorporating the Product Life Cycle Model, an organization can understand the various trends and drivers that they are embattled with and by leveraging the Cyber Threat Intelligence Services the organizations can determine how these threats are being materialized through different tactics, techniques, tools and procedures. Such actionable intelligence provides Organizations valuable insight to develop their products or workflows with the principle of Security by Design & Security by Default.

WORKFLOW - ADDING CYBER THREAT INTELLIGENCE AND PRODUCT LIFE CYCLE MODEL IN RISK MANAGEMENT



Another example of leveraging Cyber Threat Intelligence in Risk Assessment appears when there is a need for Quantitative data relevant to at least Sustained & Critical Trends mentioned above.

On Underground forums, the stolen information, assets, access to networks and servers is sold by various threat actors. These purchase costs in numerical values provide further insights to Information Security Risk Professionals to ascertain the value of their assets, assets equivalent in nature, potential costs of varying levels of attacks etc.

These gaps in the numerical values observed between intrinsic Impact estimations and the ones reported by Cyber Threat Intelligence allow you to revisit your estimation process and examine if estimations were calculated due to misperceptions as I mentioned earlier.

A specific example can be of Credit Cards Data getting traded on underground forums and various shops. Such intelligence provides insight on the value of your credit cards and the potential loss due to fraudulent transactions due to exposure of such data, it can allow risk management function to evaluate the cost associated with the re-issuance of new cards to their customers and through a comprehensive risk analysis, a proper selection of control can be made.

CONCLUSION

As I mentioned that Risk Management is a Lynchpin, a cornerstone that sets apart individuals, societies and organizations from others. However if it's done in an offhand manner or in silos then the entire Risk Management Process itself becomes a vulnerability.

An effectively functioning Cyber Threat Intelligence Program can help Risk Management Function in creating threat-centric risk scenarios. Once the risk scenarios are established, Cyber Threat Intelligence can further aid in risk estimations. This active involvement of Cyber Threat Intelligence function equips the Risk Management in making informed decisions and smart budget allocations to support overall the business goals and objectives.