**Understanding the need for cyber risk quantification**

With the growth of new technologies and an increase in new approaches, security is a top risk to all organizations. Between the high-profile breaches and regulatory scrutiny, it is seen that most companies are focusing on security more than ever. This implies that the security professionals are being asked by the board and the executive team to more clearly and crisply articulate the risks of the organization.

**What is cyber risk quantification?**

Quantitative cyber risk measurement is when time is taken out for tested models and approaches in risk management which is applied to cyber security. It is the process that calculates all the exposed risks and the impact they can make on the business environment. It drives alignment between the objectives concerning business and different security strategies. What it does is it allows the professionals to probabilistically model the risks that the organization faces in real business terms. In a recent study of fertility conducted by the thought labs, called the cyber security imperative, where nearly 1300 organizations were surveyed, it was seen that almost 34 % of the organizations used some form of cyber risk quantification in the risk analysis determination.

**What are its benefits?**

There are many benefits of using cyber risk quantification. Some of them are enlisted below.

1. It helps in the allocation of different resources and budgets.

2. It categorizes risk based on its priority.

3. The communication and the confidence between the security and the executive leaders are improved.

4. It can track the effectiveness of different cyber security programs.

**Why do we need Cyber risk quantification?**

Cyber risk quantification is popular among cyber security professionals. The reason for its popularity is that the traditional methods which are in use are not serving the cause well enough. They are not yielding the good results that organizations need. The standard approach which is used for many years which determined likelihood and impact came up with a long list of gaps without much prioritization and is very difficult to tie back to dollars and cents. Cyber security quantification, on the other hand, allows individuals to make more informed decisions that are data-driven which has resonated with senior leaders and risk officers at some of our clients. The need came from the fact that there were many advantages and features that this method can achieve but is not accomplished by the traditional methods. These are as follows.

1)Cyber risk quantification is a more advanced way of assessing cyber risk than traditional methods that rely primarily on ordinary scales and red yellow green color scales. Because of this reason, one can speak the same language as the rest of the risk organization. One can also speak in business terms and probabilities of expected loss. This lets answer questions that were not answered before, for example, whether the cyber security risk insurance is enough for an individual or not, whether the cyber security budget is appropriate or not, etc.

2)Cyber risk measurement is not a silver bullet. It’s a useful piece of any risk framework. However, it is just a set of methods and techniques to measure risk. It does not replace the common frameworks such as the NIST cybersecurity framework.

3)Cyber security quantification detects different features like potential losses, any kind of damages if done to the basic functionality of the system, any kind of hazards faced, etc.

4)Traditional methods failed to provide optimized information against the security activities which are given by quantification. This measurement gives more accurate results and objective information.

Cyber Security technologies not only defend the organization from Cyber attacks but also work as a competitive and potential advantage for organizations. By investing in Cyber Risk Quantification, organizations can achieve Cyber maturity much faster than other organizations, and build trust with customers, partners, and vendors. They exchange critical data with the organization.

**References**

1)<https://www.metricstream.com/insights/6-reasons-why-organizations-need-to-quantify-it-and-cyber-risk.html>

2)<https://www.upguard.com/blog/what-is-cyber-risk-quantification#:~:text=Cyber%20Risk%20Quantification%20(CRQ)%20is,and%20vulnerabilities%20to%20address%20first>.

3)<https://www.protiviti.com/IN-en/technology-consulting/cybersecurity/fair>

4)<https://www.oliverwyman.com/our-expertise/insights/2019/aug/navigating-cyber-risk-quantification.html>

5)<https://en.wikipedia.org/wiki/Cyber_risk_quantification>

6)<https://www.balbix.com/insights/what-is-cyber-risk-quantification/>

7)<https://www.helpnetsecurity.com/2022/04/12/cyber-risk-quantification-impact/>