CamNorte Cyber Security Caravan: Building a Cybersecurity Framework Towards a Secured Organization

The DICT Luzon Cluster 3 held a webinar entitled cybersecurity framework via zoom and facebook live last September 2, 2021. This webinar is divided into 3 sections. First cyber security risks and frameworks overview; second is discussion about framework component; and last creating framework.

Before diving to cybersecurity discussion, the speaker defines first some terminologies in cyber security field. Some important keywords to remember are threats/cyber threats a potential incident that could harm the system or the organization. Common types of cyber threats are data breaches, natural disasters, Botnets, social engineering, insider threats, black hat hackers, mobile/IoT attacks, and malwares. Next keyword is vulnerabilities which is a weakness of an asset which can be exploited wherein it can result in the confidentiality, integrity, and availability impact. And both the vulnerability and threats can result to cyber security risk, a potential loss or damage, therefore, our ultimate goal should be keeping the overall cyber security risk low. Risk management is the identifying, assessing, responding, and prioritization of the risk to prepare, mitigate, or prevent unfortunate events.

On overview about cyber security frameworks, some common frameworks are NIST Cybersecurity Framework, ISO 27001 and ISO 27002, Control objectives for Information and Related Technologies (COBIT), and Service Organization Control (SOC2). Framework core consist of Identity (identifying assets that should be protected), protect (how to keep the asset protected), detect (detecting if someone is stealing the assets), respond (what to do if the hacker mess with the assets), and recover. Framework Tiers which describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework practices 4 tiers: Partial, Risk Informed, Repeatable, and Adaptive. And the output of the framework course/tier is called Framework profiles. Framework profile is use to identify the current and the target profile. Current profile is the ‘as is’ state of organization’s cybersecurity, while target profile is the ‘to be’ cybersecurity state. The generic implementation process of cybersecurity framework was also discussed. The process is composed of (1) Prioritizing and scope (2) Orient (3) Create current profile (4) Conducting Risk Assessment (5) Creating Target Profile (6) Determine, analyze and prioritize gaps (7) Implement an action plan.

Next topic discussed in the webinar is sample use cases of Intel Cybersecurity Framework Pilot Project and cyber security framework for manufacturing profile. On usecase #1, Intel used the NIST CSF as top level security management tool in assessing their cyber security with the goals of establishing alignment on risk, informing budget planning for risk tolerance, and communicating risk through heatmap. This project of Inter involves three people, the core group who set the target profile, validates categories/ subcategories, and performs risk assessment. The individual Security SME who scores the risk areas/ current profile. And the stakeholders and decision makers who approve the target profile, review results and set the risk tolerance level. The framework example of Intel Cybersecurity Framework shown is composed of profile they focus and tiers. The benefits of this framework provide are it foster internal discussion about various levels of risk in the organization, establish organization-specific profile based threats, vulnerabilities, and impacts the organization faces. It is also easy to understand according to the participants, it can be completed in less than 15 hours, and the tools used to develop the framework can be reused. On usecase #2: cybersecurity framework for manufacturing, it contains of framework implementation details developed for the manufacturing events. Its mission is to manage the cybersecurity risks in order to maintain environmental safety, maintain human safety, maintain production goals, maintain quality of product, and maintain sensitive information. The framework also substituted the implementation tiers with risk level: the low risk level corresponding to risk that is expected to have limited adverse effect; the moderate risk where it could be expected to have a serious adverse effect; and the high risk which is expected to have a severe catastrophic adverse effect.