Cyber threat research

Technology

Chapter 3. CYBER THREAT WITHIN THE IC ENVIRONMENT

The study uses scenario analysis which provides the best way for the DOD to adopt IC ITE as an alternative future for the possible strategic implications of the research. The scenario analysis analyzes the possible future events while considering the possible short outcomes. The possible future events depend on the quality of decision making which allow for the complete consideration of issues and their implications. The scenario analysis involves modeling the possible alternative paths.

3. 1 ICD 503

The IC ITE cannot work collaboratively well if it does not have the consent of the Direct of the National Intelligence who provides the ICD 501[1]. The ICD 501 is a risk management Framework that creates the right Practitioner Course which provides the security professional with the right skills to accomplish a given sequence of the implementing of the intelligence protocol as expected. Furthermore, the DNI provides the appropriate information systems technology for the certification and the accreditation of Risk Management[2]. In particular, ICD 501 operating under the DCID 6/3 compliance for the DCID 6/3 creates the right facing formula for the reaccreditation. The DCID 6/3 requires the proper systems of characterization based on the protective levels that are issued with the right classified information. The ICD 503 is closely related to the NIST RMF than DCID 6/3 (Nstii. com 2017). For improvement purposes, the ICD 503 was established to ensure that the Direct of National Intelligence reciprocity of various objectives. As a standard, the physical security encryption helps the

emphasis on the different DCID 6/3 standard which is part of the basic methodology.

3. 3 SECURITY VULNERABILITY

IC ITE has also requested more emphasis on the security as a way to minimize the possible attacks because of the vulnerability. The vulnerability is the general weakness of an IC ITE systems for information system security design, implementation, internal control so forth that could through accidently triggered and exploited (Dni. gov, 2017). Vulnerability assessment managed services created agencies for scanning devices that were connected to organization security for vulnerabilities. The vulnerability index creates a security measure against possible intrusion or the potential threat magnitude involved in the compromise.

3. 4 STOVE PIPE IC IT ENVIRONMENTS

The IC ITE integrates the stovepipe and silo which are used for particular information systems for intelligence while ensuring that there is a perfect collection, analysis, and production of a fully processed, analyzed and exploited to a heavier degree of data utility. The logic behind is that the efficiency of IC ITE lies on the ability to utilize a certain form of intelligence. The exploitation enhances the precise information security system while recreating the right knowledge protocols that are necessary for the technical intelligence. The 9/11 Commission Report provided by the US Congress in 2004, demonstrated in detail the inability of the CIA, FBI and US national agencies if they did not have the right intelligence, hence under stovepiping allowed for the effective intelligence decentralization[3]. However, the stovepipes maximize on the secrecy gave that they help in proving when a

system is dysfunction and lacks the right resources during implementation. The stovepiping dependence on the raw intelligence experiences a positive welcome based on their ability to maximize the security threshold.

3. 5 INFORMATION SHARING ENVIRONMENT

IC ITE is all about the ability of the DNI to share and integrate information between the front line federal security departments, namely, DEA, FBI, CIA, and other US national agencies. Hence, in exploring its impacts, it is notable that a high level of collaboration depends on the quality of the DNI sharing. Military organization is affected by the different environments of management. The intention of sharing information relates to the operations and the objectives which circulate various management actions. At the strategic level, the government ensures that various resources are used to achieve the expected sharing and integration objectives. The security objectives involve creating the right security framework which helps in responding to the possible threats that the government might experiences. Cisrnet (2017) describes how sharing between the security departments is important because it naturally relates to the information and the economic development of the security measure.

A close component that provides regulation of security environment is the central authority. The power can be defined to be existing control operation to influence the individual elements and people. The DNI deploys the intelligence equipment through the sequence of the various resources that are within an area of exploitation. The quality of sharing within the national environment depends on the ability to complicate the information sharing process. However, the authority might refrain from sharing the information

because it might lead to the slowing of the possible national objectives[4]. The government seeks to abstain from the exchange of information based on the compromise created for sharing information and the national goals that should be achieved proactively. In sharing, there are international bodies such as the NATO that come as permanent stakeholders that improve the limited capabilities based on different political goals.

3. 6 HELPING ANALYST

The IE analyst uses some different graphical tools that help in reigniting various security measures. In IC ITE security, these tools help in drawing the picture while equipping the analyst with the desired information. These tools are designed, and assist in analyzing a more productive method of that required accomplish flexibility between the lists of security departments. The approach is more productive for achieving and assuming the appropriate course of description while identifying the immediate improvement. The operation process involves describing the proper standard for operation of the footstools and the unconventional operation while performing heart surgery[5]. The service method adopts the right chart symbols which include creating the right subdivision process and the changes in the modification process. The inspection procedure involves verifying whether the quality standard was observed. Through the two approaches, the roles of the analyst can be easily be defined.

3. 6. 1 What’s in it for the Analyst?

The DNI analysts works within the specific requirements related to the involvement and the difference between success and failures. The analysts

explore the project success and the position while determining the procedure for the analysis and the commodity which is more reflective of the process of review. The analyst depends on the quality of existing technology which facilitates various IT oriented measures. The organization invests more in the areas and the relationship of management for the project management which involves determining the procedures of ITE infrastructure. Also, based on the growing number of security measurements required, there should be a solid case of investing in IT. The analysts should therefore understand

· Scope of the Systems - This is naturally the environment that surrounds the business about the vision and of the organization

· Interpreting business needs - Determining the business analytical procedure which relates to the stakeholder requirements for development while translating the different questions for the business

· Explaining technical issue - Determining the business environment as well as the professional situation surrounding the business while appreciating the measures that the firm is adopting

· Project details - Determining the business analytical work for the project while ensuring that the fast process, business rules, and the requirements grew proactively.

· Putting the team together. The analyst will require working closely with the other team members to ensure that he connects creatively with each stakeholder.