The Intelligence Cycle as a tool for effective Information Security infrastructure design

Carlos Francisco Lerma Reséndez
Research Associate. Strategic Intelligence Academic Group. Graduate School of Public Management (EGAP).
ITESM
Monterrey, Mexico
cf Lerma@gmail.com

Abstract—Information Security infrastructures contain information that originates from an organization’s day-to-day operations, is stored for current or future use and whose nature tends to fall into different categories. Because of the fact that virtually all organizations have grown to depend on their internal information systems to operate and take decisions, this information has to be safeguarded in order to assure its three main properties: Confidentiality, integrity and availability. Once this need is identified by an organization, the main challenge is the adequate planning and successful deployment of an InfoSec infrastructure, which are processes that are often prone to errors that lead to defective solutions, wasted resources and an increasing risk of information theft, destruction, alteration and unauthorized dissemination. The main concept addressed in this paper is the use of the Intelligence Cycle (IC) as a design tool that helps an organization to correctly assess the risks that the organization is facing; the InfoSec resources at hand and the ones that it needs, the way it will allocate these resources in order to put them to work for the benefit of the organization and the way it will monitor this infrastructure in order to assure a proper level of protection.

Keywords—Strategic intelligence, information security, information technology, information assurance, threat management.

I. INTRODUCTION

Nowadays, most organizations rely on Information Technology (IT) to process and store all the information that is generated and handled inside them. The size, nature and origin of the data, as well as the organizations that handle/process it, can be described and catalogued using a wide range of criteria. Organizations can range from small businesses to large-scale companies and government agencies that make use of complex systems.

The information inside such systems may be freely accessed by anyone that is a part of the organization or it may be only accessed by only a few people and given special treatment because of its confidentiality, in which case, it might be classified using access permissions based on how sensitive the data is and how many users or groups can access it. When it comes to the origin of data, it can be produced internally and take many forms (documents, spreadsheets, databases, web pages, images, sound clips, videos) or it could be generated externally and enter the organization through different ways.

Having identified information as the main asset to be protected in any IT infrastructure, the goal of every InfoSec initiative is to provide the highest level of protection possible according confidentiality, integrity and availability. In order to provide a quality InfoSec service, an organization must:

1. Identify the services and assets that must be safeguarded, assigning them values according to their importance.
2. Identify internal and external threats to the most valuable assets in the IT infrastructure as well as existing vulnerabilities.
3. Establish the information needs that the IT organization has in order to know what type of information must be collected, analyzed and disseminated to provide an early warning against attacks.
4. Integrate a combination of hardware, software and administrative resources that form the backbone of the InfoSec infrastructure.
5. Establish the allocation of the InfoSec hardware and software resources (mentioned in the previous step).

Once the main asset and goals of the InfoSec infrastructure are defined, the final part of the problem lies in the need of a tool that provides direction for InfoSec practitioners in order to fulfill the steps mentioned above. The proposed solution is the integration of the Intelligence cycle as a design-oriented tool. The Intelligence cycle helps define the elements needed to establish successful processes such as requirements definition and information-related activities such as gathering, processing, analysis, dissemination and utilization. A great advantage of integrating the cycle as a is that it is not vendor-specific and is not technology-related, which makes it flexible and versatile. InfoSec practitioners can apply it to a design problem without having to think about specific brands or technologies.

II. DEFINING THE CYCLE

In order to understand the Intelligence cycle, it has to be defined thoroughly to know its composition and purpose. The cycle can be defined as a "systematic and ethical process of
gathering, classification, analysis and dissemination of operable knowledge, focused towards decision makers, so that they can take preventive or corrective measures with the highest possible level of rationality”¹. In this definition there are a number of characteristics that are particularly important:

1. **Systematic**: Several parts are chained together in a predefined sequential order. They also handle a specific input (information) and produce a specific output (intelligence, or “operable knowledge”).

2. **Ethical**: It is intended to be used in a responsible and non-malicious way. An important aspect of the integration of the intelligence cycle with InfoSec is that it is entirely defensive, preventive, corrective and design-oriented and not considered for offensive or illegal activities (“black hat”-oriented).

3. **Operable knowledge**: Operable knowledge is information that has meaning and can be used towards achieving a main goal. In the case of InfoSec, operable knowledge has design and prevention uses.

4. **Focused towards decision makers**: Operable knowledge produced by the Intelligence cycle is intended to reach individuals that take decisions. These individuals may fall into a wide range, spanning from upper management down to InfoSec analysts, platform and network administrators.

5. **Preventive and corrective action**: The Intelligence cycle produces operable knowledge that aids key elements of InfoSec. The effect of this information is preventive (effective platform design, risk assessment and resource allocation) and corrective (threat analysis, traffic pattern analysis, root-cause determination).

6. **High-level rationality**: The application of the Intelligence cycle helps produce information after going through extensive analysis, including all possible scenarios and outcomes. This is the main element that allows decision makers to avoid unforeseen events that might affect their courses of action. The phrase “surprise is not acceptable in intelligence environments”² sums up this aspect of the cycle.

### III. ELEMEENTS OF THE CYCLE

Tello & Villarreal’s definition of the Intelligence cycle provides an interconnected set of activities that must be planned, executed and managed to produce operable knowledge that aids decision makers. The parts of the cycle must be separated in order to understand their nature and purpose but also to identify which parts of an InfoSec infrastructure fall into the corresponding Intelligence cycle activities to assure proper planning of the infrastructure, which includes all the resources that will be allocated.

---


The use of automated tools to retrieve information are quickly gaining acceptance among InfoSec practitioners as they save considerable amounts of work and time. Splunk, which is a product mentioned above, is worth mentioning in specific because it is able to retrieve a special type of information known as machine data", which is generated by IT and network/telecomm equipment in a native form and is easily manipulated through a reporting console. Also worth mentioning is the proliferation of External information produced by InfoSec enthusiasts as these sources put expert knowledge at the service of InfoSec practitioners.

VI. ANALYSIS AND PRODUCTION

Intelligence analysis can be defined as “A formal process which attempts to find and measure relations among variables. Although at times it may draw heavily on mathematics and numeric procedures, it is a logical and not a mathematical process”. Intelligence analysis promotes a unique way of thinking that integrates possible scenarios or complements incomplete information with data that might have been isolated but is linked because of specific characteristics. This phase of the cycle is very extensive and its study can extend entire decision making. In order to establish a reference that can link this phase to InfoSec, a number of analysis techniques are explained along with possible uses:

<table>
<thead>
<tr>
<th>Technique</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission</td>
<td>Moving data from one point to the other.</td>
<td>1. Sending users information on safe use of computers using email distribution lists. 2. Sharing information between platform administrators and InfoSec administrators regarding a specific issue.</td>
</tr>
<tr>
<td>Accumulation</td>
<td>Storing data in one place; implies some notion of retrievability.</td>
<td>1. Construction of knowledge bases (KBs) that store cases and procedures regarding InfoSec incidents. 2. Keeping InfoSec configuration diaries that illustrate specific ways of setting up equipment.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Many data points brought together into a smaller set which is usually more easily accessed.</td>
<td>1. Use of reporting tools like Critical Watch that can trim the number of events and produce a simplified vulnerability report. 2. Integration of specific data from different platform into custom reports designed by purpose-specific InfoSec analysts.</td>
</tr>
<tr>
<td>Analysis</td>
<td>Dissection of data, usually formal, of data in order to seek and measure relations.</td>
<td>1. Use of data collection selection tools that identify possible threats based on readings and indicators. 2. Use of methodologies like COBIT to map out specific vulnerabilities areas of an InfoSec infrastructure.</td>
</tr>
<tr>
<td>Mix</td>
<td>Passing of data around to a variety of managers looking for possible links. The data is often not well ordered.</td>
<td>1. Creation of task groups for the solution of issues that require IT and InfoSec joint cooperation. 2. Determination of Operating System hardening procedures by IT and InfoSec analysts aimed to prevent external attacks.</td>
</tr>
</tbody>
</table>
The introduction of Security Information and Event Management (SIEM) systems has been proven valuable as tools that integrate information from different sources but also correlates and tracks relationships to provide answers once a threat has been identified. A SIEM system is a “complex collection of technologies designed to provide vision and clarity on the corporate IT system as a whole” that can be assembled either as an out-of-the-box solution or as a custom development. InfoSec analysts can use these systems to recognize patterns and behaviors of the IT infrastructure to avert an attack or prevent one.

VIII. CONCLUSIONS

The use of the Intelligence cycle as a design tool for effective InfoSec environments is geared towards the eradication of common mistakes made by organizations that face the challenge of building an InfoSec infrastructure from scratch or want to improve an ailing or ineffective one. The greatest advantage that this tool provides is its vendor and technology neutrality: The ability to look at the conceptual part of the problem without involving specific technologies or manufacturers provides a solution that can be adapted to the needs of any organization without any interoperability or integration problems. The use of the Intelligence cycle can be considered a logical step in an InfoSec environment because of the defensive nature of both and also because they both try to integrate assets, information and people into a cohesive unit that can generate valuable information and action geared towards the protection of an underlying element.

REFERENCES


