MEASURING SECURITY EFFECTIVENESS

David Israel, cissp\(^1\), Rahamim Yosef\(^2\)

Motorola
16, Kermenitzki St, Tel-Aviv, Israel
\(^1\)Tel: 972-3-5659465 David.Israel@motorola.com
\(^2\)Tel:972-3-5658220 cyr001@motorola.com

Abstract

Over the years, organizations have been implementing various security systems and controls in order to solve their security risks and enable their business processes.

The existence of many security systems and processes is very important for the organization, but does the organization know if its security systems are effective? Are the security tools and processes doing what they are supposed to do? Do they have tools to decide if security is improving?

This document will try to define how security professionals can measure security effectiveness based on the security systems that are in use.

Security definition and the organization risks

The classic security definition is: Confidentiality, Integrity, and Availability (C.I.A). The three fundamental principles of information security are translated into implementation of many organization security processes and systems in order to safeguard business risks.

Each of the three (C.I.A) includes many business risks, with the same threat caused by a variety of different potential security breaches.

For Example:

Confidentiality can be jeopardized by:

- Data leakage (mail, flash memory, ftp, http)
- Unauthorized access
- Privacy violation
- Unencrypted confidential data
- Trojans

Integrity can be jeopardized by:

- Unauthorized data changes
- Lack of Segregation of duties (fraud)
- Operational incidents

Availability is influenced from:

- BCP/DRP plan
- Backup
- Virus Outbreak

We can see that an organization's security status is a combination of many inputs from all of the security tools and processes. This makes the overall security effort spread over many safeguards, with a limited ability to see the whole security picture. In order to figure out the global security status, we have to understand what happens in each and every one of the security operations. (By using the term "security operation", I would like to include any security tool, process or control whose purpose is to reduce business security risk)

To be able to do this we need to start measuring security operations that will become the building block for understanding the global security status.
**What to measure?**

First we need to define some basic parameters for each security operation.

For each operation, define the following:

What do you want to measure: choose measurable security issues that can be counted and can give valuable information regarding the security status managed by this operation.

Baseline value: The baseline, starting point of the operation you want to measure.

Goal value: Define the desired value you want to achieve in order to bring the specific operation to an acceptable level or risk.

Current value: Obtain the current value at time of measure.

Having the above parameters will give us the information that we need to calculate the specific security operation status which is, in fact, the operation's effectiveness.

Effectiveness formula (1)

\[
\text{Effectiveness} = \frac{\text{ABS} (\text{Current Value} - \text{Baseline})}{\text{ABS} (\text{Goal} - \text{Baseline})}
\]

So, for example, if we would like to measure the effectiveness of the organization's security patch distribution, we can easily get a clear understanding where we stand on achieving the required goal.

<table>
<thead>
<tr>
<th>Security Operation</th>
<th>What to measure?</th>
<th>Baseline</th>
<th>Goal</th>
<th>Current Value</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Patch distribution</td>
<td>Time to full implementation</td>
<td>14 days</td>
<td>7 days</td>
<td>10 days</td>
<td>57.14%</td>
</tr>
</tbody>
</table>

**Rate the risk**

When we know how to evaluate single security operation effectiveness, we can then apply the same principle for the entire measurable security operations that safeguard each one of the business risks.

These are the building blocks for creating an effective view of the organization security risk status in terms of Confidentiality, Integrity, and Availability.

In order to be able to score the effectiveness of the organizations confidentiality operations, we need to assign weights for each operation included. In this way we can also calculate each relative score, and then the total score for the entire security risk.

For example, if organization A has 3 security operations that deal with confidentiality, each one get its weighted share on the global risk and each gets its relative score.

The global score of confidentiality operation will be the sum of the relative score.

<table>
<thead>
<tr>
<th>Org. A - Confidentiality operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security operation</td>
</tr>
<tr>
<td>Laptop encryption deployment</td>
</tr>
</tbody>
</table>
In this case, organization A has poor performance on confidentiality operations, but it has a tool to put the finger on the exact reasons.

**Total security effectiveness.**

Doing the same process for the C.I.A business risks can give the organization an important and accurate view of its security effectiveness status, derived from many security inputs that exist on the organization security infrastructure.

It is clear that the total score of security operation effectiveness is an important input for understanding the organization security risk. If the security operations receive a low score, it means that security tools, controls and tasks are not functioning as they are supposed to, security investments are not paying back; and corrective actions clearly must be taken.

Unlike Security Information Systems (SIM), that can reflect the current security status by analyzing online security events from a computing environment, the method of calculating the total score for security operations effectiveness is more like an indicator for symptoms that can create a serious security incident.

If organization A is, for example, a very large law firm, the main business risk would be its customers' confidentiality, therefore when rating the C.I.A risks it would receive the highest weighting between the three.

Its total security risk may look like this.

<table>
<thead>
<tr>
<th>Security Risk</th>
<th>Eff.</th>
<th>Weighting</th>
<th>Relative score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>52%</td>
<td>60%</td>
<td>31.2</td>
</tr>
<tr>
<td>Integrity</td>
<td>70%</td>
<td>20%</td>
<td>14</td>
</tr>
<tr>
<td>Availability</td>
<td>80%</td>
<td>20%</td>
<td>16</td>
</tr>
<tr>
<td><strong>Total Score for Security operations</strong></td>
<td><strong>61.2 %</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Since organization A has defined that Confidentiality is the highest business risk, its total score is very much affected by the low score achieved on the Confidentiality operation effectiveness.

Now we can create the final view of the security operations effectiveness in terms of risk level. The higher total score you get, the lower risk exists for the business.

Below is an example for security "health" indicator divided to 3 risks level.
Scorecard

Since this method is based on gathering timely information from many systems and processes, we have now an excellent infrastructure for creating a scorecard for all our security operations.

We can create a visual presentation of the process by showing the collected data. The scorecard can show changes and trends by relying on historical data. It can show the current state, goal and baseline with the time and budget factor.

The target audience for scorecards can be anyone in the organization that is involved and interested in this kind of information. Consider the CISO, CIO, internal auditor, regulatory compliance auditor, IT operations manager, and even the CFO when budget has a critical influence on the results.

Special Attention

There are 2 main drawbacks on measuring security effectiveness process. One is the definition of the measurement subject, and the other is the data collection process.

In order to define "what to measure" we must carefully choose processes that are measurable and have parameters that can represent a real security issue. We don’t want to measure irrelevant operations that might mislead us from analyzing the real security state we are in.

Once the processes are defined we need to establish clear reporting processes and create an automated report and data collection process (it can use the SIM system if available, or simply create some scripts or database queries). Data must be auditable and repeatable in order to avoid inaccurate results.

Summary

Measuring security effectiveness as described in this article is a MUST tool for security professionals and decision makers. Only by creating the overall picture of the organization security operation status, with the ability to drill down for the root cause, can an organization improve its security and reduce business risks.

Bibliography

Measuring Security Effectiveness – Pete Lindstrom, Elizabeth Nichols, RSA Conf Feb2006