@ISACA Volume 14 13 July 2016

In This Issue

Five Useful Information Risk and Security Metrics

SHARE

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

It is difficult to improve what cannot be measured. Information risk management and security programs are maturing beyond their basic capabilities. They now provide a wide range of services to their organizations. Inevitably, both the leaders who run these programs and the organizations they serve want to measure and monitor the programs' performance to ensure they are meeting their expectations and requirements. There are many measures and metrics that can be used, but the following 5 are often useful since they are both objective in nature and their value can easily be understood by a wide range of audiences:

1. **The number of information security-related events and incidents identified**—There is a clear distinction between information security events and incidents. Events are activities or indicators that warrant further investigation and can be indicators of incidents. Incidents occur when a material event or events have occurred and require a formal response activity. These 2 data points can be used for trend analysis and other intelligence-related activities, especially when they are categorized, e.g., ransomware, physical security, malware/virus or data breach.

   A significant increase in events and incidents can provide the organization valuable insights about its attractiveness to adversaries and the level of concern it should have. If an organization experiences a sustained increase in events and incidents, it is important to identify if this occurred due to improvements with detection and response capabilities or through an increase of interest and targeting by adversaries.
2. **The number of newly identified and previously existing validated information security-related vulnerabilities**—The identification of new vulnerabilities can demonstrate progress in increasing visibility to information risk within the organization and enumerate exposures that need to be addressed. Newly identified vulnerabilities should be reported separately from existing vulnerabilities. This will differentiate them and potentially identify aging concerns for remediation activities associated with previously identified vulnerabilities.

   Prior to being reported, it is important that the identified vulnerabilities are validated and appropriately classified (e.g., critical risk, high risk, medium risk, low risk) for the potential risk they pose to the organization. This will ensure the measurements being presented are viewed as valid concerns and not an attempt by risk and security personnel to introduce fear, uncertainty and doubt (FUD) to promote an agenda.
3. **The elapsed time from vulnerability identification to completion of remediation activities**—Once a vulnerability has been identified and validated, the organization is at greater risk, not only from the exposure to the vulnerability, but also from how long it takes to address it. In this situation, the organization transitions from a position of ignorance about the vulnerability, which is often easier to excuse, to one of negligence, which is harder for an organization to defend (if it is determined that the organization did not remediate the vulnerability in a commercially reasonable time frame). If the vulnerability to be exploited and the resulting consequences triggered litigation, a compliance concern or a regulatory finding, there will likely be an examination of the level of effort and remediation activities that were applied by the organization. The intention will be to identify how well the organization managed and remediated the exploited vulnerability both before and after the incident occurred.

   This information can also be useful in helping an organization measure the effectiveness of its vulnerability management program and capabilities. Using trend analysis, an organization can examine the efficiency with which it is remediating vulnerabilities compared to its current and future goals and expectations. A trend of continuous improvement will demonstrate positive progress and efficiency within the program. A trend of extended remediation times can be an early warning to the organization's leadership about its ability to effectively manage information security-related vulnerabilities.
4. **The number of information security policy exceptions requested and granted**—A key performance indicator for the effectiveness and acceptance of information security policies is the frequency and rate that security policy exceptions are both requested and granted. If information security policies are new or have recent changes, it is typical to see a higher rate of exception requests and approvals. This is typically due to time and resource requirements needed for compliance. However, this can also be an indicator that the organization is not yet capable of adopting the policies or their effective dates were not properly planned. Ideally, there should be a reduction in the number of exception requests and grants within a short period after the effective dates.

   Situations in which there are numerous policy exception requests and approvals for reasons other than initial introduction are often an indicator that policies are not appropriate for the organization. Information risk and security leaders can review these data points to identify where they may need to revisit policies to ensure alignment with capabilities, ability for implementation and expectations of the organizations they are attempting to govern using these policies.
5. **The number of customer information risk management and security inquiries received and the level of effort required to respond to them**—Customer information risk management and security inquiries, such as questionnaires, have become a common practice for many organizations. Responding to these questionnaires is important for customer relations, but it can also be time-consuming and resource-constraining due to the level of effort involved. By identifying the number of inquiries and the level of effort associated with the responses, information risk and security leaders have objective data points they can use to justify their need for additional support (e.g., funding, resources, systems). When the inquiries have a direct correlation to customer satisfaction and retention or sales, there is often a higher likelihood of positive outcomes since these inquiries are attached to profit instead of cost centers.

   The number of inquiries and level of effort required to respond to them can also help identify trends in customer expectations and requirements. If the number of inquiries and level of effort are consistently growing, it would suggest an increased interest and expectations in the organization's risk and security capabilities by customers. It is often useful to identify what areas within the inquiries (e.g., network security, application security, encryption, incident response) are growing or becoming more specific, which can be a useful input to strategy development and investment planning activities.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.

Learn Through Hands-on Training at CSX 2016 North America Conference