"Make Information Security Events Operational Anomalies: Being Proactive Pays Off"

By: John P. Pironti, CISA, CISM, CISSP
Enterprise Solutions Architect/Security Consultant
Unisys Corporation
Viewpoint
February 2005

Information security is a pervasive challenge to businesses and government. It must be approached in a proactive and programmatic way if we are ever to gain control of the problems and mitigate the security risks that threaten information infrastructure.

Information security events can no longer be treated simply in a reactive fashion, where the organization responds to an attack or event. Information security is a business imperative. It must be built into an organization's operational DNA. If we wait for the attack or event to happen then the adversary has won and the organization has been compromised.

We also cannot rely solely on technology to solve the problem. Technology must be treated as a tool to implement a business process, procedure, or methodology to solve the security problem.

Currently most organizations attempt to overcome information security challenges by implementing heroic efforts with highly skilled and specialized teams. Those specialists' services are costly because they rely on high levels of expertise and require significant resources to be effective. Those teams also tend to be technical in nature and do not necessarily appreciate the business problems that the solutions they are working with are designed to solve. Without a clear understanding of the business need and activity, these teams might cause more harm than good to the organization.

The complexity of business solutions will grow steadily as we continue to leverage information infrastructure successfully in the future. Organizations have begun to expand their borders, extending them to include partners, vendors, and customers. Those expanded borders open up new attack points for adversaries and new potential for accidental user activities to cause security events that can affect the information infrastructure not only of their own organization but also of the extended enterprise.

In this new environment, the traditional model of responding to attacks and events as they happen will no longer be acceptable in this model.

Information security now requires a proactive approach.

The best way to do that and approach information security proactively is to introduce a program aligned to the business goals of the organization. This program utilizes a

structured and measurable approach to provide information security capabilities to an organization. Two key elements are threat and vulnerability assessment and vulnerability management and incident response. Those two elements represent the fundamental shift to a proactive approach to information security from a reactive one.

Threat and Vulnerability Assessment

Threat and vulnerability assessment includes analyzing and assessing the severity of threats to an organization's information infrastructure. These threats can be both internal and external in nature, and the approach to them will be both proactive and reactive.

The proactive elements are designed to help an organization use a threat analysis methodology to understand the current and emerging risk to its information infrastructure. This methodology will take into account the business goals and objectives of the organization and will be repeatable across all solutions in order to ensure consistency within the framework.

The reactive elements are those designed to provide the management team and decision makers within an organization with an understanding of the immediate threat posed by active attacks. They will be given an educated analysis of the likelihood, severity, and potential business impact of different attacks or security-related events. This will allow them to appropriately align resources and capabilities to repel the attacks and properly manage communication streams and expectations within the organization.

The primary goal of the threat and vulnerability assessment element of the program is to provide the organization with a proactive approach to risk management. This approach enables alignment to the business objectives and goals of the organization and presents information in a way that is useful to the business elements of the organization as well as to the technical elements.

(Insert Figure 1.0)

Incident and Vulnerability Management

The incident and vulnerability management function contains both a proactive and a reactive element as well. The proactive element gains input from threat and vulnerability assessment function, as well as from other sources, to understand what vulnerabilities exist and the risk they pose within a particular solution or the organization as a whole. This function then is responsible for implementing controls and measures to mitigate the risk posed by those vulnerabilities.

One way the vulnerability management function can accomplish that goal is by creating plans in advance for response to events and attacks against the identified vulnerabilities within the solution. These response plans include prescriptive guidance on identification and appropriate response. The function can then forward those identification and response plans to the operations organization through a link that can include the

identification and remediation steps within automated monitoring systems, electronic defenses, and incident response systems.

The reactive role for incident and vulnerability management covers traditional incident response activity. In this role this function is responsible for remedying malicious activities that are hindering the organization's ability to function appropriately. There's difference in this case, though: the incident response team now becomes the second-tier of response in case of an incident, because the primary role is now handled by the operations teams.

The incident response element will be invoked only when the specific incident has not previously been identified and an appropriate response plan created for use by the operations teams. The incident response team may also be invoked when the response plan that was created does not work appropriately, or the operations team does not have the appropriate resource pool available to execute the response plan effectively.

Regulatory Compliance

There are currently information security elements to multiple regulations with which global organizations must comply, such as the Gramm-Leach-Bliley Act, Sarbanes-Oxley Act, Basel II, and the European Data Privacy Directive, among others. All can have a significant impact on how organizations maintain the security and integrity of their information assets. These regulations were put in place to maintain at least baseline standards for organization in situations where previously there had been little if any uniformity in processes.

Final Thoughts

Organizations have not been protecting themselves effectively against malicious adversaries or information security incidents created by user error. As information becomes more valuable to enterprises and governments and their potential antagonists, more regulation will be enacted to ensure even higher levels of security.

The introduction of an information security program aligned to leading industry practices and methods enables an organization to achieve compliance with both current and future information security regulations.

A proactive information security program also allows an organization to make mature risk management decisions by providing a business-friendly context for discovery and extension of its security capabilities. This permits business leaders to understand how their organizations can withstand security events and the impact that those events can have on the organization's ability to function.

The transformation to a proactive environment from a reactive one enables the organization to gather and control the data necessary to identify threats and take preventive measures before it can become the victim of a malicious or accidental

security breach. And with that improved security posture can come significant collateral benefits: lower operational costs, greater efficiencies, and minimized risk to brand, reputation and other precious business commodities.

Figure 1.0