Web Traits, Inc.
9423 Eagleton Lane
Montgomery Village, MD 20886
Bhaskar Roy and Ragu Nathan

Effective System Security Needs Trusted Partnership

Trends in System Security

Not a single week passes by it seems, without news items on information system security breaches making it to the national headlines. Organizations both small and large from public and commercial sectors appear to suffer such embarrassing breaches no matter how well prepared they are. To the skeptic public, and even sympathetic information system professionals, organizations with information systems appear to exist only in two states: have been hacked or soon to be hacked. In addition, the threats to our information system have emerged rather rapidly. We are quite sure that nations with armies of professionals dedicated to exploiting vulnerabilities in our systems for political reasons have been added to thrill seeking hackers exploiting them for inexplicable psychological reasons. On the positive side, the resources available to secure our systems have also grown rapidly. The laws, regulations, guidelines, standards, best practices, tools, techniques, reliable databases of vulnerabilities, general awareness and vendors with specialized skills, all intended to protect our information systems, continue to grow at an amazing pace.

Challenges Faced by Executives

Executives entrusted with securing information systems have access to both a rapidly growing list of resources to help their cause and details of ever-emerging threats. Web Traits, Inc. works with many such executives on information assurance, vulnerability assessments, certification & accreditations, network monitoring and traffic analysis, FISMA compliance, cloud computing, security operation centers, disaster recovery and business continuity and risk management.

Executives typically are supported by our team of system security professionals who maintain right levels of expertise and knowledge of current trends. These professionals provide timely and reliable system security related data to the executives. System security data related to organizational vulnerabilities, risks and compliance are essential components of what is made available. Current system security data from the outside world are also added to this. Hence more often than not, an overwhelming amount of data is continuously made available to the executives. They still have many reasons to be concerned as reports of breaches from the outside world are quite frequent and never conclusive in their root causes. Each executive we support also faces organizational issues that impede pro-active measures for system security. We assist many federal agencies, as their executives constantly assess the means and options, to stay prepared for the unexpected and prevent the undesired.

Independence in Security Services

Faced with numerous challenges and negative reports of security breaches in adjacent organizations, system security executives resort to building an information security program tailored to their organizational structure, prevailing security postures and existing risks. Elements of a good system security program are well defined, published and practiced. A critical attribute of a security program, that we wish to focus on, is the need for independence in the assessment of information system security weaknesses and the risks posed by them. This independence is not an easy objective when most system security activities are conducted by an organization's own employees. The reporting structure of the organization tends to

interfere in the much needed independence of the system security tasks and its findings. This independence is a non-trivial objective even when the services of outside vendors are utilized for an organization's system security tasks. Armed with the right expertise, a vendor will frequently convey not-so-pleasant messages about organization's security posture to its key executives. Even the very executive that hired the vendor may not always react positively to the frequent reports on weaknesses and vulnerabilities.

Need for Trusted Partnership

The independence of system security tasks may warrant further explanations. Nearly all system security tasks are directly or indirectly related to the assessment of an organization's weaknesses, vulnerabilities, risks and mitigations. When such assessments are objective in nature, based on verifiable facts, the value of the resulting actions enhances the system security posture of an organization. As opposed to this, an organization that depends on biased security assessments (Such as influenced by personal relationships, confidence, optimism, vendor's business interest or other aspects) are operating in a vulnerable situation. They have spent significant resources on security tasks and yet, are in effect operating their information systems without a reliable measure of weaknesses and risks. They also have no credible mitigation strategies as well. Hence, for a security service vendor to be effective in enhancing an organization's system security, it is imperative that they practice objective fact based assessment and report the weaknesses, vulnerabilities, risks and mitigations, in a timely manner. The executives will act on a vendor's findings only if they trust that the vendor has acted as an independent un-biased assessor and reporter of security attributes. The vendor in turn needs to trust that the executive accountable for system security will continue to support the assessments, even if they should result in reports of additional weaknesses and vulnerabilities. Such independence has been in practice for financial audits for many decades now. Yet when it comes to system security services this is still left to a trusted relationship between an organization and its security service provider. Hence a trusted partnership with a qualified vendor is essential for an effective system security program of any organization.

Conclusion

Independent assessments that determine an organization's weaknesses, vulnerabilities, risks and mitigations are critical to an organization's ability to protect against growing threats to their information systems. A trusted partnership with a vendor who can offer such system security services is essential to the success of an executive in charge of system security.

To learn more about the importance of independent assessments and trusted relationship in system security services contact Bhaskar Roy at Bhaskar.Roy@web-traits.com or Ragu.Nathan@web-traits.com.