Security Program Reviews:
Security in Practice

Anthko
Cyber Security

November 21, 2018

Introduction

Often when organization hear they are going to be audited they ensure they have all the correct paperwork prepared in all the correct ways. Security audits were never intended to be designed to ensure organizations are creating good security programs on paper so why are auditors allowed to short change organizations with inadequate reviews and recommendations? Organization leaders should demand more, leverage the auditors' independent perspectives, and ensure the results and recommendations are accurate and relevant. In this document we discuss what a proper security program audit or review (these two words are used interchangeably,) should include, how to properly leverage the independence of the auditors, and the best ways to determine if the results are accurate and relevant.

Demand More

Many times, an audit will consist of the audit team sitting in a small room and asking an organization's delegation for various documents and artifacts without ever seeing any process or control in action. Then, once the audit has been completed the recommendations will be to create a new policy, process document, or procedure. These types of audits do not help the organization's leaders gain transparency blind spots in their programs or fulfill the true purpose of the audit. Organizational leaders should demand that auditors actually review the processes and settings in use to determine the security program in action and not just on paper. When security auditors measure security in practice with an independent point-of-view they can bridge the gap between the organization's documented security program and implemented security program. These insights can then be leveraged by organizational leaders to identify any gaps.

Leverage the Independence

One of the main attributes of a competent auditing organization is their independence. Without independence it could be easier to over look "small" infractions or gaps between the organization's security requirements and implementations. This is especially true when the offender has a position of great authority or is greatly liked by peers. Business leaders should leverage this unique independence to gain extremely valuable insights into their programs. When we look in a mirror we tend to have a distorted self-view. Many organizations see their security posture as much more secure that a competent auditor may for many reasons. Auditors have a great breadth of knowledge or many security programs across many organization and have learned to spot recurring weaknesses that are not always self-evident, threat actors' techniques and tactics change the risk landscape, and media focus on one area of cyber security may distract organization leaders from other areas. Using a proven framework and true independence, competent security auditors can help organization leaders see these potential problem areas and make accurate and relevant recommendations.

Review Results

There have been occasions where organization leaders have provided auditors with all of the requested artifacts that were requested, had very little to no feedback during the review, then were surprised with results and recommendations that recommended changes that were already in use or that were not relevant to the organization. This is a failure on the part of the auditors to include the organization throughout the review process. Auditors should perform many self checks (sometimes called “sanity checks,”) throughout the review process, to ensure results accurately reflect the security program in practice. Organizational leaders should plan periodic meetings with auditors to discuss progress, potential problem areas, and potential areas of success. When reviewing the recommendations, organization leaders should ensure the recommendations accurately reflect the organizations security in practice by being supported by security in practice artifacts and observations, and are relevant to the technologies and business offerings of the organization.

Summary

Security in practice should be the focus of any competent auditor, not security in documentation. This may be a significant shift from traditional audits in which organizations have traditionally participated; however, this will assist in finding gaps between organizations’ documented security program and the security program that is being exercised. Organizational leaders should embrace the independence auditors have and resist the urge to limit this independence to ensure an accurate picture of the environment is fully painted. As results are delivered, organizational leaders should review the results to ensure they are accurate based on security in practice artifacts and relevant based on the organization’s resources, capabilities, and business offerings.

Connect with us

please visit us at AnthkoCyberSecurity.com to learn more about our organization, to see our service offerings, or contact us.