SUBROSA

CYBER SOLUTIONS

Cybersecurity Maturity Assessments

subrosacyber.com

Cybersecurity Maturity Assessments

Even if organizations have a cybersecurity program in place, it can be challenging to prioritize and protect critical assets, infrastructure and applications in an ever-changing landscape. While you might believe your company's data is secure—how do you really know if your organization has enough fortifications to defend against your biggest threats?

By employing a security program assessment, organizations can examine how well-developed and comprehensive your cybersecurity defense posture truly is. The details of the assessment may differ depending on who is conducting the test, but the main purpose of a security program assessment is to gauge the effectiveness of current procedures.

Why should your organization run a security assessment?

1. To build a case for augmenting cybersecurity

Oftentimes, information technology (IT) specialists will use the findings of a security assessment to make a case for enhancing an organization's current program. Analyzing these types of reports will show board members or key stakeholders involved in key decision-making processes that new expenditures or infrastructure is needed. Having data-backed evidence that underscores an argument to augment your cybersecurity even further will allow your organization to combat cyber-crime in a more effective, holistic manner.

2. To ensure cybersecurity is 'top of mind'

In *an article by Infosecurity Magazine*, more than 52 percent of breaches reported in 2017 were a result of actual hacks, while 15 percent were due to lack of security software and another 11 percent occurred because there weren't enough internal controls in place to prevent employee negligence. While enacting fundamental protections is a critical part of any security program, maintaining a cybersecurity-inclined frame of mind is important for every employee year-round. Employing a security assessment will make your staff more conscious of cybersecurity issues, making them less likely to fall for scams or basic mistakes that lead to breaches.

3. To discover weaknesses in your system

One of the most common reasons why organizations run security program assessments is to discover potential weaknesses in your current cybersecurity system so that they can be remediated. By examining all of your IT assets, such as security policies, software programs and operating systems, it will be possible to recognize glaring issues in your defense posture. Knowing your weaknesses will allow you to prioritize and implement recommendations based on the security assessment's reports.

SubRosa Cyber Solutions can conduct a comprehensive security program assessment that covers all bases. After collecting and reviewing information from your organization, conducting interviews with your staff and communicating the most critical issues, you can begin to effectively implement recommendations to improve your overall security posture.