7 STEPS TO THOROUGH CYBER SYSTEMS TESTING

Taking a proactive approach to cybersecurity is far less costly than dealing with the aftermath of a cybersecurity breach. In addition to the reputational harm that could result from a breach, cybercrime is expected to cost a total of $6 trillion globally by 2021, according to Cybersecurity Ventures. Assessing your cyber risk is mission critical, and it goes far beyond a compliance audit. What steps can you take to thoroughly test your systems for cyber risk?

1. CONDUCT A COMPREHENSIVE RISK ASSESSMENT

Take a look at the functions of your business that contain the most valuable assets—and this doesn't just include sensitive customer or business data. Consider your operations and where business disruption would be damaging. For instance, not all hackers are financially motivated, they may want to halt your supply chain to limit productivity. Once you've laid out all areas of risks—from financial to operational and reputational—you can begin to tackle them one-by-one based on your business goals.

2. ADMINISTER A PENETRATION TEST

Do you know where your network infrastructure and information systems exposures are? To safeguard your cyber systems, you have to find the hacker's way in. If a hacker can locate a single means of entry or bypass security features, your entire system is vulnerable. Simulate attacks against your network to discover unknown weaknesses, both internally and externally. However, keep in mind this test ends once a single point of entry is found, leaving the possibility open for other unknown exposures.

3. RUN A VULNERABILITY SCAN

At a bank, the vault may be the main prize, but it's not the only consideration. You need to be strategic about security guard placement, exit surveillance and bank drawer protection. A comprehensive vulnerability scan is critical to allow you to zoom out to view the full layout of your organization's systems and test each potential access point and weakness. Then pinpoint the right patch.

BDO

4. ORDER AN EMAIL SYSTEM CYBER-ATTACK ASSESSMENT

Two of the most notable cyber-attacks in recent history, WannaCry and NotPetya, were launched via malicious email. Given the dramatic growth of cyber attacks that take place through email, an in-depth, advanced diagnostic assessment of an organization's email system is essential. These separate tests can detect complex persistent threat malware, which may otherwise go undetected.

5. IMPLEMENT A SPEAR-PHISHING CAMPAIGN

Have you ever received a frantic late-night email from your boss? Now imagine a hacker is actually behind that email, posing as your boss. Spear-phishing attacks are highly targeted attempts to secure sensitive information and have proven effective. It's vital to assess the level of cyber awareness of your organization's employees at all levels to reduce instances of human vulnerabilities.

6. SCRUTINIZE YOUR VENDORS

Even if your organization's systems are protected, all of your outside vendors—from trading partners and B2B connections to maintenance vendors and catering services—are also access points. Third-party relationships should be viewed as an extension of your business and held to the same standards. Make sure each vendor has the appropriate level of access to your data and that their data privacy policies and compliance practices are examined.

7. REASSESS, RINSE, REPEAT

Cyber risks change and mature as quickly as technology does. To maintain secure systems, it's critical that you continually assess cybersecurity controls and conduct these tests on an annual basis—and this is not a project strictly for the CIO or IT function. Protecting your business from catastrophe is a shared responsibility. It's contingent upon proper communication of cybersecurity strategies and plans, and an in-depth understanding by the board, management and any business leaders charged with oversight.

Thorough cyber systems testing is a substantial undertaking. Do you have the resources to do it yourself? A System and Organization Controls (SOC) attestation can help you find and close gaps in cybersecurity controls and add credibility to your risk management program.

CONTACT

JEFF WARD
Third-Party Attestation – National Managing Partner
314-889-1220 / jward@bdo.com