# Why Security Testing Makes Good Business Sense:

# 3 Benefits to Your Organization

Provided by Security Vitals

SECURITY VITALS

ENTERPRISE DATA SECURITY ANALYTICS

# Why security testing makes good business sense

Think you're safe…think again.  The unfortunate reality is that any business is a target for cyberattacks.  While many smaller businesses want to believe they are not on the attacker's "radar" the truth is they are.  In fact, small and mid-size companies are often targeted because of their perceived weak defenses as well as their access to larger firms.  This dangerous combination makes them a focal point for malicious players seeking an easy payday.

The odds are stacked against any company that does not proactively look for areas an attacker could exploit. If your firm is one of them…the cost of doing nothing can be staggering.   With average data breach recovery costs eclipsing $8 million, it's easy to understand why a proactive testing to identify security gaps makes good business sense.

# Staying ahead of the curve

So, the real question is…would you like to identify vulnerable areas before the attackers do? Conducting security testing on the company network (penetration testing) is a proactive measure that should be an integral component of annual business planning.

The reasons are simple.  Growing any business requires a delicate balance of risk/reward, and the more insight a leadership team has on risk, the more equipped they are to mitigate it. As such, penetration testing is an activity that bears strategic consideration at the business planning level and ongoing execution at the tactical planning level.

# How it works

Network Penetration testing is a process of identifying the IT assets connected to a company network, highlighting security gaps, and demonstrating what type of attacks could cause an adverse impact to the business.  In most cases, an information security firm is retained to conduct the testing as they can provide an unbiased third-party evaluation. The testing is done with automated tools and can be enhanced with manual intervention from consulting resources. As testing is conducted observations, gaps, and mitigation recommendations are documented as part of the final deliverable.

While many consider the testing process to be a technical evaluation, be careful not to overlook the broad business ramifications. Since the business (and underlying technology) is always evolving to support growth and market changes, it is important to schedule one or more test each year. The 2020 Ponemon Institute Research Report reported that "58% of organizations find that every recurring penetration test finds a new, vulnerable or high-risk pathway into their organization." A recurring testing approach helps identify evolving risk and provides the necessary feedback on how to address it.

# What you get

The main goal of any security test is to improve insight and knowledge…ultimately to highlight areas that represent risk to an organization. It is important to note that not every test will result in broad risk revelations. In the case of testing, the process of embracing it is just as important as the results. Alternatively, if your organization doesn't conduct testing, you will never know about potential threats that could shut the company down. Conducting penetration testing on an annual or semi-annual basis offers benefits for organizations large and small:

**Cost Effective**
penetration testing is a relatively low-cost service that can completed and delivered in weeks

**Third-Party Validation**
helps the organization uncover risk that internal resources may not know about

**Risk Insights**
the data collected during a penetration test increases awareness and knowledge of evolving risk; also delivers the details on how to effectively mitigate it

Effectively managing cyber risk requires an ongoing blend of technology and process. Penetration testing is one of many effective tools for mitigating risk. For organizations that want to embrace a proactive stance, penetration testing is a solid means of validating where it exists and how it can be addressed. Most of all, it provides the peace of mind that you have taken an important step toward protecting your organization's information assets.

# Security Vitals Can Help You

Security Vitals offers testing options that are tailored to the individual needs of clients.

**Schedule a Discovery Call Today**

securityvitals.com | (866) 802-9405 | sales@securityvitals.com

SECURITY VITALS
ENTERPRISE DATA SECURITY ANALYTICS