LAYER SOLUTIONS INC.

WHY RISK ASSESSMENTS are Non-Negotiable

Merely adding disparate security solutions to your network isn't enough to protect your business from a security disaster if you don't know the risks your business faces – not just today but in the long run as well.

What a Security Risk Assessment Entails

A security risk assessment involves identifying information assets that might be targeted by security threats (internal and external), assessing your business' network and data security posture, and gauging threats (prevalent and imminent) to your information assets.

THE STEP-BY-STEP PROCESS

STEP 1:

Determine the value of an information asset

Formulate a mechanism to determine the importance of an asset in your network.

STEP 2:

Prioritize assets

Identify the assets to evaluate and determine how they would be assessed.

STEP 3:

Identify threats

List down any threat, such as natural disasters, system failure, human error, adversarial threats and others, that could harm your business.

STEP 4:

Assess vulnerabilities

A vulnerability is any weakness that a threat can exploit to breach your business' security and wreak havoc.

STEP 5:

Analyze existing controls

Analyze the checks and balances already in place to minimize or eliminate the probability of a threat.

STEP 6:

Document the entire process

It is both a best practice and a mandate under several regulations to ensure that the entire risk assessment is thoroughly documented.

STEP 7:

REPEAT ALL OF IT AGAIN, REGULARLY.

LAYER SOLUTIONS INC.

Non-Negotiable

Although a single assessment may demonstrate that your business is safe, please do not assume it will remain safe indefinitely. Given the growing vulnerabilities at your business and the ever-evolving threat landscape, it is nothing but smart business to ensure you conduct risk assessments regularly, document them meticulously and carry out remediation efforts.

Here's what you can achieve by devising an ongoing security risk assessment strategy:

Keep Threats at Bay

Mitigate prevalent and potential threats while keeping vulnerabilities such as user-related risks, third-party/supply chain risks and Dark Web exposure risks at bay.

Prevent Data Loss

Adopt a more proactive approach to tackling any possible attempts at compromising your business data.

Enhance Operations

Assure your workforce that their hard work will not vanish into thin air. Boosting the morale of your employees will in turn enhance their productivity.

Reduce Long-Term Costs

Save your business significant revenue and/or potential reputational damage by identifying security leakages and plugging them in time.

Improve Organizational Knowledge

Maintain an organization-wide knowledge base of network and asset discovery, vulnerabilities, network changes and areas of improvement.

Avoid Regulatory Compliance Issues

By putting up a formidable defense against security threats, you will automatically avoid hassles with respect to complying with regulatory standards such as HIPAA, GDPR, PCI DSS, etc

Set Yourself Apart

Stand out amid competition as an organization capable of instilling greater confidence in clients and customers by demonstrating that your business is determined to keep security intact.

Don't Handle This Alone

Seek a trusted partner to ensure risk assessments are thorough and accurate so you get the precise insights you need to act decisively against security threats.

Contact us today to learn how ongoing risk assessment and management isn't really an ordeal when done the right way.