CADENCE CYBER

info@cadence-cyber.com

813-546-4646 Cadence-Cyber.com

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 STEPS AGAIN, REGULARLY.

Cadence Cyber

info@cadence-cyber.com 🔒 813-546-4646 🔒 Cadence-Cyber.com

WHY RISK ASSESSMENTS are NON-NEGOTIABLE