NuHarbor

Make cybersecurity easier

www.nuharborsecurity.com

4 Steps to a Rock-Solid Cybersecurity Strategy

STEP 1

Ask and Understand

- **Business Alignment.** Identify core business functions enabled by technology.
- **Tolerance for Change.** Assess the organization's readiness and willingness to adapt to security measures.
- **Future Plans.** Learn about plans to change technology or vendors on the roadmap.
- **Identifying Supporters and Challengers.** Identify supporters and resisters of your security ideas.

STEP 2

Apply Your Expertise

- **Take stock of threats, vulnerabilities, and risks specific to your organization.** Determine what threats, vulnerabilities, and risks are specific to your organization.
- **Determine Controls.** Create a comprehensive list of security controls, policies, and operational measures.
- **Collaborate.** Engage with other departments and stakeholders to understand their perspectives.
- **Educate and build consensus.** Educate others about the importance of security recommendations and involve them in decision-making.

STEP 3

Measure Progress

- **Continuous Monitoring.** Regularly review and assess the effectiveness of security controls.
- **Engage Stakeholders.** Collaborate with security teams and make sure everyone knows their roles.
- **Dependencies Matter.** Be aware of dependencies between security measures.

STEP 4

Create and Communicate

- **Documentation.** Document your cybersecurity strategy, including controls and procedures.
- **Transparency.** Maintain transparency by reporting progress regularly.
- **Engagement and Consensus.** Continuously engage with stakeholders and maintain consensus.

BONUS

Continuous Improvement and Adaptation

- **Regular Assessments.** Conduct periodic assessments and audits of your cybersecurity strategy.
- **Threat Intelligence.** Stay updated on cybersecurity threats and trends.
- **Technology Evolution.** Assess the effectiveness of existing security measures against new technologies.
- **Training and Awareness.** Implement ongoing cybersecurity training and awareness programs for employees.
- **Incident Response Planning.** Continuously refine the incident response plan based on lessons learned.
- **Regulatory Compliance.** Stay updated on cybersecurity regulations and compliance requirements.
- **Communication.** Maintain open communication channels with stakeholders.

Need help with your security strategy? Learn more here.