CYBERSECURITY

5 Steps to Cybersecurity Risk Management

Combine process, technology, and training to mitigate risk and ensure compliance.

1

Inventory your assets.

Determine your most valuable data assets, as well as the impact on your business if such information became unavailable or stolen. System outages or hacking efforts can result in lost time, revenue, and reputation.

2

Identify threats and vulnerabilities.

Use scanning tools to identify software and network vulnerabilities, and consider who might exploit them for entry. Potential hackers include competitors, disgruntled employees, and cyberterrorism groups. Keep in mind, even loyal employees can accidentally damage information or share it with the wrong people.

3

Profile and **mitigate** risks.

Taking assets, threats, vulnerabilities, and safeguards into account, decide which risks can be tolerated versus those that need further countermeasures. Develop countermeasures by weighing the potential impact and likelihood of a risk against the cost of effective protection.

4

Implement processes and training.

For each risk requiring additional protection, document your rationale. Train your employees on risks and countermeasures on an ongoing basis to ensure compliance and competency.

5

Update your cybersecurity program.

Hackers and technology are constantly advancing. Stay ahead by regularly assessing threats, testing vulnerabilities, improving countermeasures, and updating training.

Next Steps

Experts Can Help

Cybersecurity Audit

Cybersecurity Improvement Plan

Security Awareness Training