Vanta

Risk assessment 101

Performing a risk assessment

01

What is a risk assessment?

A security risk assessment identifies, assesses, and implements essential security controls in your company's applications. It aims to find areas within your organization that need additional or stronger security.

02

Why should I perform a risk assessment?

43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves. Breaches can cost a company millions of dollars. An effective risk assessment strategy can improve your security posture, and protect your company's most valuable data and information.

43%

of cyber attacks are aimed at small businesses

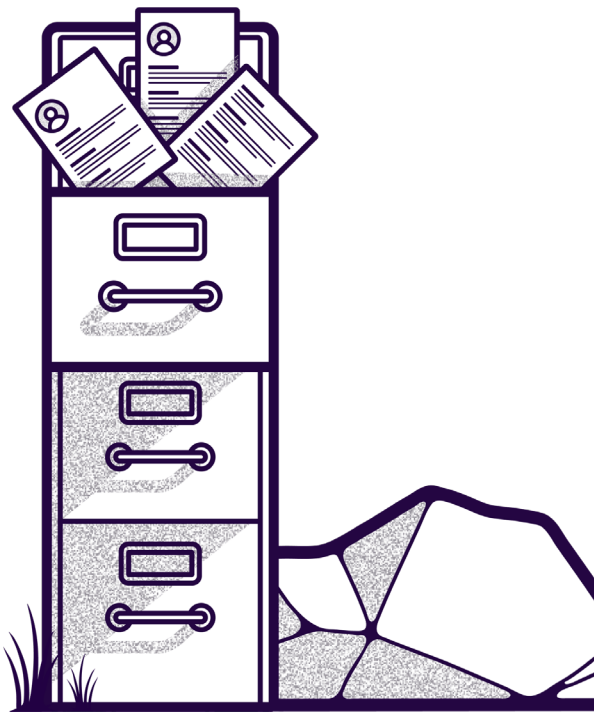
14%

are prepared to defend themselves

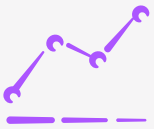
03

When should I perform a risk assessment?

Once a year, or before a company merger, before a company acquisition, or deploying new technology.



Where do I start?



Identify asset inventory and the value of each asset

Identify vulnerabilities and threats

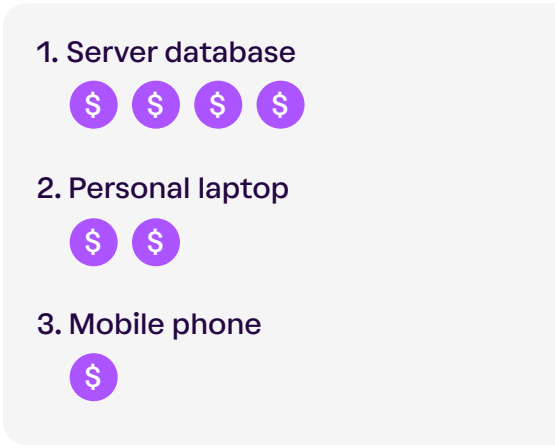
Threat probability & impact

Threat impact and the cost of protecting your assets

Understanding risk assessment

Asset inventory & value

A company server database server has **more value** than most personal assets such as a personal laptop or mobile device. If a server was hacked, it would be much more detrimental to the company than a personal laptop, giving the server a higher value. Performing an asset inventory will help you understand what is on your network, and allow you to prioritize **protecting your high value assets.**

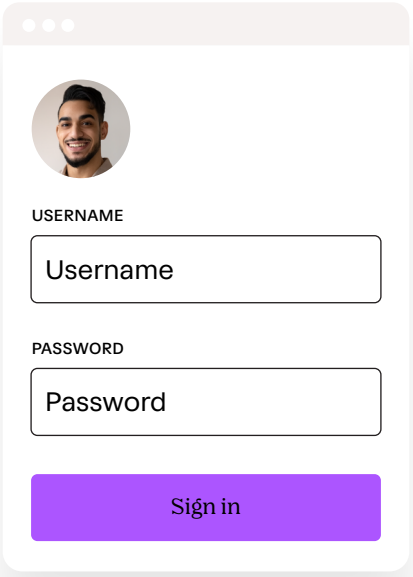


Identify vulnerabilities and threats

A vulnerability on an asset can be exploited. Patching and remediating your vulnerabilities with high risk scores limits the potential for a breach.

What makes a vulnerability high risk?

A high risk vulnerability is easy to exploit and requires minimal effort. For example, if you use a platform with default login credentials (ie, USERNAME: Username, PASSWORD: Password) this becomes a known and **easily exploitable** vulnerability. If your platform admin forgot to change the default credentials, a hacker with very limited experience could access your information using the default credentials.



Threat probability & impact

How likely is it that this threat will occur, and how much damage will it cause?

If a vulnerability is extremely challenging to exploit and requires an expert hacker to execute, the risk is less likely to occur. Additionally if the exploit wasn't detrimental to your operations (ie, the exploit would not interfere with sensitive data) the impact would be less.

If a vulnerability is extremely easy to breach with novice hacker skills and would provide access to client credit card information, the threat probability is high, and the impact is high. These are the risks to prioritize first.

For a more comprehensive understanding of Vulnerability Scoring, take a look at the National Vulnerability Database.

Threat impact and the cost of protecting your assets

Determine the prioritization of your assets, the vulnerabilities found within your network and what needs to be done to protect them. High risk assets should be a priority spend because they would pose a higher risk to your organization if breached.

Establishing a risk assessment framework

Are there any specific compliancies the organization is trying to achieve? (SOC2, HIPAA, GDPR, etc.)

Each compliance has a framework of policies that are required to be monitored and assessed.

What can be done to create a risk assessment framework structured around compliance?

- Perform company wide security training
- Employees receive targeted training relevant to their role
- Managers meet with direct reports weekly to review their work
- Managers are responsible to mentor and provide guidance to increase staff awareness of security policies
- Leverage tools that detect and alert asset misconfigurations and vulnerabilities

Risk assessment and vulnerability management is a continuous cycle.

1. **Discover**

   What assets are available?

2. **Assess**

   How Valuable are these assets to our company, and what vulnerabilities have we found on them?

3. **Report**

   What have we found, who should be involved, and what is our plan moving forward?

4. **Remediate**

   Take action and fix the issues.

5. **Verify**

   Confirm vulnerabilities have been patched, and compliances are met.

6. **Repeat the cycle!**

Vanta

Vanta is the easy way to get and stay compliant. Thousands of fast-growing companies depend on Vanta to automate their security monitoring and get ready for security audits in weeks, not months. Simply connect your tools to Vanta, fix the gaps on your dashboard, and then work with a Vanta-trained auditor to complete your audit.

Request Demo →

VANTA.COM