safous

How To Assess Your Cybersecurity Risk

A WORKBOOK

Is your cybersecurity up to date? Complete this workbook to see where your security posture is lacking and learn how to keep your business network and critical assets protected.

Why conduct a cybersecurity risk assessment?

Cybersecurity risk assessments can help you better understand how to protect your company's vulnerable IT assets – a must in the ever-evolving threat landscape. **Use this workbook to ask yourself key questions designed to help you identify gaps and growth opportunities in your company's cybersecurity strategy.**

How Secure Is Your Business Network?

Even the most secure organizations can fall victim to cyberattacks.

Hackers find new ways to infiltrate corporate networks daily, so no organization – large or small – is ever 100% safe from cyberattacks. Luckily, you can help protect your company by taking proactive steps toward strengthening your security posture with a risk assessment.

Why do you need a cybersecurity risk assessment?

Here are four reasons:[1]

65,000+
network vulnerabilities were discovered in 2022.

Hackers will steal an estimated **33 billion** records this year.

The average total cost of data breaches is **$4.35 million.**

47%
of all U.S. businesses suffered a cyberattack last year.

1. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

QUESTION #1:

What are your essential systems and processes?

Identifying the processes your business needs in order to operate is a critical first step when assessing your cybersecurity posture.

Use this section to list the systems your business relies on to function, even at the most basic level. For example, this could include a program that receives payments, an application used to access customer data, or IoT devices that must remain accessible to the public.

Critical system #1:

Critical system #2:

Critical system #3:

Critical system #4:

Secure Your Most Important Systems

Keep operations running, if only at the bare minimum.

To get the most value from your DIY risk assessment, start by defining the systems critical to your company's essential functions. By identifying the systems that absolutely must remain accessible, you can better understand the security measures needed to ensure operations continue in the event of a cyberattack or other emergency.

QUESTION #2:

Have you taken inventory of your digital assets?

Any device or application connected to the internet can be a security risk, as cybercriminals may take advantage of these to infiltrate your network.

Use this section to take inventory of your assets. Consider everything that might be used to access your company's information, including hardware such as desktops, laptops, and smartphones, and the various applications your employees use to perform work duties.

Hardware:

Software:

Data Storage:

Identify Your Vulnerable Assets

Discover which assets – physical and digital – need better protection.

As remote and hybrid work models become the new workplace standard, unsecured public networks and personal devices expose more corporate networks to data breaches. But because businesses lose over $1 million more on average where remote employees are a factor in a breach,[2] keeping track of your company's digital assets is essential for ensuring you have the security controls to protect them.

2. https://www.ibm.com/security/data-breach

QUESTION #3:

What security measures do you currently have in place?

Now that you've identified your company's critical systems and digital resources, it's time to examine how you protect them.

Use this section to identify your current cybersecurity practices and determine which areas need stronger security measures to become more effective.

How are user identities managed?

- [ ] Individual accounts
- [ ] Shared accounts

How secure are your passwords?

- [ ] Combines upper and lowercase letters, numbers, & symbols
- [ ] At least twelve characters
- [ ] Changed every 180 days
- [ ] Not reused from the last six passwords
- [ ] Lockout after unsuccessful attempts

What security tools are in place?

- [ ] Data encryption
- [ ] Firewalls
- [ ] Authentication controls
- [ ] Browser isolation
- [ ] Identity and Access Management
- [ ] Email Security
- [ ] Secure Web
- [ ] Cloud Security
- [ ] SaaS Security
- [ ] End Point (EDR/Anti-malware)
- [ ] XDR/MDR
- [ ] DLP
- [ ] Threat Intelligence
- [ ] Firewalls, WAF, WAAP

How is OS and application patching handled?

- [ ] Automatically
- [ ] Manually
- [ ] N/A

Strengthen Your Security Posture

Identify vulnerabilities and opportunities for improvement.

When done correctly, your risk assessment can help you identify gaps in your current cybersecurity strategy, such as unpatched software, weak passwords, and other potential risks. By determining where your current security measures are lacking, you can implement stronger solutions to ensure your network stays safe now and in the future.

QUESTION #4:

What are your third-party risks?

Providing too much privileged access to third-party vendors and contractors can increase risks such as data breaches or the introduction of malware into your network.

Use this section to take inventory of your third-party risks. Consider all third-party users, the level of network access they're permitted, and which controls you have in place to manage them.

Third-party user accounts:

Permissions provided:

Authentication controls:

Minimize Your Third-Party Risks

You can't control third parties, but you can control their network access.

54% of businesses lack a comprehensive inventory of third-party access to their network.[3] Minimize your company's third-party risks by identifying your third-party users and putting measures in place to limit access if an account is compromised.

3. https://www.forbes.com/sites/forbestechcouncil/2021/11/03/why-managing-third-party-access-requires-a-better-approach

Improve Your Cybersecurity Posture With Safous

Safous can help you keep your business network safer than ever.

If you haven't conducted a cybersecurity risk assessment lately, it's time to make it a priority. Now that you've gotten a better idea of your vulnerabilities, Safous can help you shore up any gaps in your security to keep your network safe at all times.

Contact us today to learn more about how a Safous Security Assessment can help you protect your business.

Visit Safous.com to learn more.