YES, YOU NEED A SOC FOR CYBER REPORT – HERE'S WHY

Cybersecurity threats aren't just increasing in number — they're becoming more dangerous and expensive as well.

Cyber attacks affect organizations around the globe, but the most expensive attacks occur in the U.S., where the average cost of a data breach is $9.44 million, according to IBM's 2022 Cost of a Data Breach Report. The same report shows that the cost of a breach is $10.10 million in the healthcare industry, $5.97 million in the financial industry, $5.01 million in the pharmaceuticals industry and $4.97 million in the technology industry.

Cyber threat actors are a serious danger to your company, and your customers, stakeholders and shareholders know it. They expect you to be prepared to defend against and manage cybersecurity threats.

How can you demonstrate your cybersecurity controls are up to par? By obtaining a SOC for Cybersecurity report.

WHAT IS A SOC FOR CYBERSECURITY REPORT?

It provides an independent assessment of an organization's cybersecurity risk management program. Specifically, it determines how effectively the organization's internal controls monitor, prevent and address cybersecurity threats.

WHAT'S INCLUDED IN THE REPORT?

The report is made up of three key components:

1. **Management's Description** of their cybersecurity risk management program, aligned with a control framework (more on that below) and 19 Description Criteria laid out by the AICPA.
2. **Management's Assertion** that controls are effective to achieve cybersecurity objectives.
3. **Service Auditor's Opinion** on both management's description and management's assertion.

WHY SHOULD I CONSIDER A SOC FOR CYBERSECURITY REPORT?

A SOC for Cybersecurity report offers several important benefits for your organization, which include:

- **Align with evolving regulatory requirements.** The cybersecurity regulatory environment is constantly evolving. In particular, the SEC's cybersecurity guidelines are becoming stricter over time. A SOC for Cybersecurity report can demonstrate you're aligned with these guidelines. If you're a public company or are considering going public in the future, you need to be prepared to meet not just the SEC's guidelines of today, but their evolved guidelines in the future.
- **Keep your board of directors informed.** Your board is responsible for ensuring the business is effectively addressing and mitigating risks — and that includes cyber risk. A SOC for Cybersecurity report offers your board a clear and practical illustration of your organization's cybersecurity risk management controls.
- **Attract and retain more customers.** It's becoming increasingly common for companies to require that their vendors have a SOC for Cybersecurity report. Even for companies that don't require such a report, it's important to know their vendors are keeping their data safe. Having this report differentiates you from vendors who have not prepared one.
- **Improve your cybersecurity posture.** A SOC for Cybersecurity report can identify current gaps in your cybersecurity risk management program. Once you've addressed these gaps, you can show your customers, stakeholders and shareholders that you're continuously improving and evolving your cybersecurity risk management approach.

HOW DO I PREPARE FOR MY SOC FOR CYBERSECURITY ASSESSMENT?

There are several steps you should take to prepare for your assessment.

- **Choose your control framework.** You have several options, including the NIST Cybersecurity Framework, ISO 27002 and the Secure Controls Framework (SCF). There are multiple online resources to help you choose the framework that's right for your organization.
- **Determine who your key internal stakeholders are for your cybersecurity risk management program.** You'll need to select a point person to be responsible for ensuring the independent services auditor has all the documentation they need to complete their assessment and act as liaison across internal and external stakeholders.
- **Collect all cybersecurity-related documentation in one location.** Make sure you have an organizational system that makes sense to your point person so it's easy for them to pull the appropriate materials to give to the independent services auditor.
- **Conduct a readiness assessment.** You can work with an independent services auditor to conduct such an assessment which will identify gaps you can address before performing the attestation.
- **Select an independent services auditor to perform the attestation.** SOC for Cybersecurity services are provided by independent CPAs approved by the AICPA. Ideally, you'll want to select a firm that is experienced in your industry, has a diverse and robust team of cybersecurity professionals and is accessible when and where you need them.

HOW CAN BDO HELP?

Once you've determined that you're ready to obtain a SOC for Cybersecurity report, BDO can help you:

- Assess your organization's current cybersecurity risk management program
- Conduct a readiness assessment and gap analysis
- Recommend remediation strategies
- Perform the SOC for Cybersecurity attestation

BDO offers SOC for Cybersecurity services across industries, with a specialized focus on government contracting, financial services, technology, healthcare and media. When you work with BDO, you get access to one of the world's largest global networks of professionals.

READY TO DISCUSS YOUR SOC FOR CYBERSECURITY REPORT? Click here to get started ▶