5 Questions Every CISO Should Ask Themselves

As a CISO your work never stops. When you're not reviewing and defining cybersecurity policies, drawing up disaster recovery and continuity management plans, or preparing for the next round of regulatory audits, you're handling urgent risks in real time and solving issues as they arise. Here are five questions to help evaluate and improve your organization's cybersecurity.

How are you structuring your organization's data?

Strong, scalable, and intuitive data organization is one of the most important facets of any good DLP strategy. Is your data taxonomy content or context based? How would you explain your reason behind the way your data is structured to an employee? By applying data security best practices and being able to communicate your logic in a succinct manner you're both continually self-auditing and ensuring your strategy fits the needs of the people within your organization. Speaking of other company members...

How are you working to increase employee buy-in?

To use a cliche, "a chain is only as strong as its weakest link." You can have the best cybersecurity system in the world but if someone in Accounting or Human Resources downloads the wrong file at the wrong time you're in big trouble! With this in mind, how are you working to keep your employees up to date on modern developments in the cybersecurity ecosystem? Are you conducting refresher sessions, or working with organization members on effective internal data protection? On the topic of threats...

What threats are on the horizon?

The best professionals in every industry are constantly studying developments in their fields, and you should be too! In a rapidly changing sector like infosec risks often aren't identified until they've been exploited. With the rising prevalence of 0-day attacks and more stringent SEC cybersecurity reporting regulations in the works, proactivity is the best way to prevent data breaches. Keep an eye on social media to stay up to date on all reported attacks (like our LinkedIn!), and new reports from the Cybersecurity and Infrastructure Security Agency (CISA).

What are your highest risk targets?

Understanding what information controlled by your organization that hackers would be most invested getting their hands on is a great way to determine how you should allocate your resources. Materials already intended for public consumption, like marketing collateral or non-sensitive press releases, might not warrant the most stringent solutions in your toolbox. Location based gating, 2FA, or more might just be more cumbersome than they're worth for less sensitive info. Valuable data, like personal employee data stored by HR, or deal information from the finance team, should be protected by every tool you have at your disposal! Understanding what data is the most valuable will help ensure you're putting your energy into what makes the largest impact.

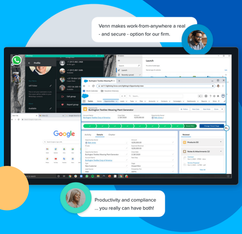
Are your security solutions impeding employee productivity?

Cybersecurity is paramount for any successful organization in our modern business climate, but unfortunately many existing virtual desktop solutions are cumbersome and prevent employees from working to their full potential. In fact, according to a recent Venn/Harris Poll study, 71% of employed Americans have navigated around their company's IT policies to be more productive at their job. That's a massive risk! Audit your solutions, and make sure your tools aren't so clunky that they're incentivizing employees to circumvent them. Speaking of streamlined solutions...

LOOKING TO ENABLE BYOD ACCESS & SECURE YOUR ENDPOINTS?

Venn is a game changing secure workspace, helping your organization isolate and protect work data from any personal use on the same computer. It's a simple, turnkey solution that enables BYOD without compromising on security.

It's time to give your remote teams the best.



BOOK A DEMO TODAY →

GET IN TOUCH!
marketing@venn.com | venn.com

venn