**7 Tough Cybersecurity Interview Questions**

Cyber security analyst. Information security specialist. Software security engineer. Chief information security officer. No matter where your interest lies in cybersecurity, [your skills are needed](https://cybertalentnetwork.org/2019/01/08/5-hands-on-cybersecurity-skills-in-high-demand/). All that stands between you and your dream role, is the job interview.

When meeting with organizations ready to fill cybersecurity positions, you should be prepared to face some tough questions. Employers will want to gauge your practical knowledge, as well as determine whether you can tell the difference between some key cybersecurity concepts (i.e., black hat, white hat, and gray hat hackers). Here are a few questions you can expect to encounter during the interview process.

**1. Why did you (or do you) want to get involved in cybersecurity?**

Your credentials may demonstrate where you’ve been and what hard skills you’ve developed, but they won’t necessarily show your passion for the cause and your gumption for fighting cyber criminals. Be ready to [talk about your strengths in the intangible areas](https://cybertalentnetwork.org/2019/01/08/10-most-desired-traits-for-cyber-security-job-candidates/) of instinct, sense of duty, morality, and such.

**2. Can you describe a time you solved a cybersecurity issue within a team?**

[Soft skills are sorely needed in cybersecurity](https://cybersecurityventures.com/jobs/), including being able to work as part of a team. Effective cybersecurity means having to solve problems with others, so being able to bring to mind times when you’ve worked as part of a group will be essential. A potential employer will want to know that you can play nicely as a team member, along with being able to critical-think on your own.

Be aware that this may lend itself to another question about any roadblocks you might have encountered while solving a cybersecurity concern. It’s best to highlight how you took positive action within the team, or even led the team, to overcome something such as individual differences of opinion, varying skill levels within the group, or management intervention. Just be careful in discussing how you overcame any management issues so as not to put off an executive-level interviewer.

**3. Have you ever experienced a serious breach?**

While talking about your problem-solving skills within a team atmosphere, be prepared for this hard-hitting question. [Jason Taule](https://www.linkedin.com/in/jason-taule-67267b/), vice president of Standards and CISO at HITRUST, considers this one especially tough because there is no right answer.

“No one wants to admit to having had a breach on their watch, but many times they happen despite one’s best efforts through no fault of the security team or CISO,” Taule says. “On the other hand, a ‘no’ response might suggest the candidate lacks necessary experience to successfully navigate an organization through a major breach.”

Taule’s suggestion: Acknowledge the seeming inevitability of breaches, “but focus on accomplishments in building successful detection capabilities and effective incident response programs, and describing experiences gained handling less severe but otherwise reportable events instead.”

**4. How do you stay on top of industry trends and changes?**

This question is designed to test your industry knowledge. Is it relevant and up to date? Here, a generic answer won’t cut it. Instead, offer up some specific news websites, security forums, podcasts, or blogs, and provide an example of a recent trend and where you read about it.

This is a great time to talk about your cybersecurity education—particularly an advanced degree, and any [immersive learning experiences](https://www.cybintsolutions.com/cyber-skills-learning-works-a-case-study/) you have. You can speak about the need for constant learning in cybersecurity, and how your degree helps achieve this.

**5. What can you tell me about security within my company?**

You should definitely expect a question along these lines. It’s normal for any business to check that a candidate has researched them and understands what product or service they offer. A potential employer will want to see that you have knowledge of the type of technology they’re using and any other information you can gather.

Take it from [CSO Online’s George V. Hulme](https://www.csoonline.com/article/2134284/10-ways-to-prep-for--ndash--and-ace--ndash--a-security-job-interview.html), who advises that you should try to understand what language(s) the company uses. Anything you can offer up during an interview will add to your credibility.

**6. Can you describe a complex cybersecurity concept in easy-to-understand language?**

One of the most sought-after skills in cybersecurity is the ability to communicate a complex topic in a simplified way. As [Tim Heard at the Infosec Institute](https://resources.infosecinstitute.com/soft-skills-hiring/#gref) writes, being able to grasp the “big picture” and deliver information that’s key to specific stakeholders, while disregarding unessential information, is a highly desired trait. To build these soft skills, consider investing in a Master’s degree in Cybersecurity (if you don’t already have one) through which you can learn how to easily communicate complex cybersecurity issues and techniques.

**7. What is a pen test and can you explain the process of pen testing?**

You may not get this exact question, but as [IT security risk manager Adriano Leite](https://www.linkedin.com/pulse/40-itinformation-security-questions-worth-reviewing-before-leite/) of Cliffside Security explains, you’re likely to receive many questions about specific test protocols and be asked to take the interviewer through a specific process. Not only should you have processes like penetration testing down pat, but you should also know other types of technical details—such as encryption, basic coding, and patch management—and be able to apply your knowledge to real-world scenarios based on the level of expertise wanted. The ability to describe how you would defend an organization against a threat will be a definite plus.

When it comes to cybersecurity know-how, you can’t be too prepared for any interview question. Learn as much detail about the industry as possible, and be ready to relate everything you know back to practical examples for the interviewer.

!!!!!!!!!!!!!!!!!!!!!!!