INFORMATION SECURITY INTERVIEW QUESTIONS

General

Are open-source projects more or less secure than proprietary ones?

The answer to this question is often very telling about a given candidate. It shows 1) whether or not they know what they're talking about in terms of development, and 2) it really illustrates the maturity of the individual (a common theme among my questions). My main goal here is to get them to show me pros and cons for each. If I just get the "many eyes" regurgitation then I'll know he's read Slashdot and not much else. And if I just get the "people in China can put anything in the kernel" routine then I'll know he's not so good at looking at the complete picture. The ideal answer involves the size of the project, how many developers are working on it (and what their backgrounds are), and most importantly — quality control. In short, there's no way to tell the quality of a project simply by knowing that it's either open-source or proprietary. There are many examples of horribly insecure applications that came from both camps.

How do you change your DNS settings in Linux/Windows?

Here you're looking for a quick comeback for any position that will involve system administration (see system security). If they don't know how to change their DNS server in the two most popular operating systems in the world, then you're likely working with someone very junior or otherwise highly abstracted from the real world.

What's the difference between encoding, encryption, and hashing?

Encoding is designed to protect the integrity of data as it crosses networks and systems, i.e. to keep its original message upon arriving, and it isn't primarily a security function. It is easily reversible because the system for encoding is almost necessarily and by definition in wide use. Encryption is designed purely for confidentiality and is reversible only if you have the appropriate key/keys. With hashing the operation is one-way (non-reversible), and the output is of a fixed length that is usually much smaller than the input.

Who do you look up to within the field of Information Security? Why?

A standard question type. All we're looking for here is to see if they pay attention to the industry leaders, and to possibly glean some more insight into how they approach security. If they name a bunch of hackers/criminals that'll tell you one thing, and if they name a few of the pioneers that'll say another. If they don't know anyone in Security, we'll consider closely what position you're hiring them for. Hopefully it isn't a junior position.

Where do you get your security news from?

Here I'm looking to see how in tune they are with the security community. Answers I'm looking for include things like Team Cymru, Reddit, Twitter, etc. The exact sources don't really matter. What does matter is that he doesn't respond with, "I go to the CNET website.", or, "I wait until someone tells me about events.". It's these types of answers that will tell you he's likely not on top of things.

If you had to both encrypt and compress data during transmission, which would you do first, and why?

If they don't know the answer immediately it's ok. The key is how they react. Do they panic, or do they enjoy the challenge and think through it? I was asked this question during an interview at Cisco. I told the interviewer that I didn't know the answer but that I needed just a few seconds to figure it out. I thought out loud and within 10 seconds gave him my answer: "Compress then encrypt. If you encrypt first you'll have nothing but random data to work with, which will destroy any potential benefit from compression.

What's the difference between symmetric and public-key cryptography

Standard stuff here: single key vs. two keys, etc, etc.

In public-key cryptography you have a public and a private key, and you often perform both encryption and signing functions. Which key is used for which function?

You encrypt with the other person's public key, and you sign with your own private. If they confuse the two, don't put them in charge of your PKI project.

What kind of network do you have at home?

Good answers here are anything that shows you he's a computer/technology/security enthusiast and not just someone looking for a paycheck. So if he's got multiple systems running multiple operating systems you're probably in good shape. What you don't want to hear is, "I get enough computers when I'm at work..." I've yet to meet a serious security guy who doesn't have a considerable home network--or at least access to one, even if it's not at home.

Network Security

What port does ping work over?

A trick question, to be sure, but an important one. If he starts throwing out port numbers you may want to immediately move to the next candidate. Hint: ICMP is a layer 3 protocol (it doesn't work over a port) A good variation of this question is to ask whether ping uses TCP or UDP. An answer of either is a fail, as those are layer 4 protocols.

How exactly does traceroute/tracert work at the protocol level?

This is a fairly technical question but it's an important concept to understand. It's not natively a "security" question really, but it shows you whether or not they like to understand how things work, which is crucial for an Infosec professional. If they get it right you can lighten up and offer extra credit for the difference between Linux and Windows versions.

The key point people usually miss is that each packet that's sent out doesn't go to a different place. Many people think that it first sends a packet to the first hop, gets a time. Then it sends a packet to the second hop, gets a time, and keeps going until it gets done. That's incorrect. It actually keeps sending packets to the final destination; the only change is the TTL that's used. The extra credit is the fact that Windows uses ICMP by default while Linux uses UDP.

What are Linux's strengths and weaknesses vs. Windows?

Look for biases. Does he absolutely hate Windows and refuse to work with it? This is a sign of an immature hobbyist who will cause you problems in the future. Is he a Windows fanboy who hates Linux with a passion? If so just thank him for his time and show him out. Linux is everywhere in the security world.

Cryptographically speaking, what is the main method of building a shared secret over a public medium?

Diffie-Hellman. And if they get that right you can follow-up with the next one.

What's the difference between Diffie-Hellman and RSA?

Diffie-Hellman is a key-exchange protocol, and RSA is an encryption/signing protocol. If they get that far, make sure they can elaborate on the actual difference, which is that one requires you to have key material beforehand (RSA), while the other does not (DH). Blank stares are undesirable.

What kind of attack is a standard Diffie-Hellman exchange vulnerable to?

Man-in-the-middle, as neither side is authenticated.

Application Security

Describe the last program or script that you wrote. What problem did it solve?

All we want to see here is if the color drains from the guy's face. If he panics then we not only know he's not a programmer (not necessarily bad), but that he's afraid of programming (bad). I

know it’s controversial, but I think that any high-level security guy needs some programming skills. They don’t need to be a God at it, but they need to understand the concepts and at least be able to muddle through some scripting when required.

How would you implement a secure login field on a high traffic website where performance is a consideration?

We're looking for a basic understanding of the issue of wanting to serve the front page in HTTP, while needing to present the login form via HTTPs, and how they'd recommend doing that. A key piece of the answer should center around avoidance of the MiTM threat posed by pure HTTP. Blank stares here mean that they've never seen or heard of this problem, which means they're not likely to be anything near pro level.

What is Cross-Site Request Forgery?

Not knowing this is more forgivable than not knowing what XSS is, but only for junior positions. Desired answer: when an attacker gets a victim's browser to make requests, ideally with their credentials included, without their knowing. A solid example of this is when an IMG tag points to a URL associated with an action, e.g. http://foo.com/logout/. A victim just loading that page could potentially get logged out from foo.com, and their browser would have made the action, not them (since browsers load all IMG tags automatically).

How does one defend against CSRF?

Nonces required by the server for each page or each request is an accepted, albeit not foolproof, method. Again, we're looking for recognition and basic understanding here--not a full, expert level dissertation on the subject. Adjust expectations according to the position you're hiring for.

If you were a site administrator looking for incoming CSRF attacks, what would you look for?

This is a fun one, as it requires them to set some ground rules. Desired answers are things like, "Did we already implement nonces?", or, "That depends on whether we already have controls in place..." Undesired answers are things like checking referrer headers, or wild panic.

What’s the difference between HTTP and HTML?

Obviously the answer is that one is the networking/application protocol and the other is the markup language, but again, the main thing you're looking for is for him not to panic.

How does HTTP handle state?

It doesn't, of course. Not natively. Good answers are things like "cookies", but the best answer is that cookies are a hack to make up for the fact that HTTP doesn't do it itself.

What exactly is Cross Site Scripting?

You'd be amazed at how many security people don't know even the basics of this immensely important topic. We're looking for them to say anything regarding an attacker getting a victim to run script content (usually JavaScript) within their browser.

What’s the difference between stored and reflected XSS?

Stored is on a static page or pulled from a database and displayed to the user directly. Reflected comes from the user in the form of a request (usually constructed by an attacker), and then gets run in the victim's browser when the results are returned from the site.

What are the common defenses against XSS?

Input Validation/Output Sanitization, with focus on the latter.

Corporate/Risk

What’s the goal of information security within an organization?

This is a big one. What I look for is one of two approaches; the first is the über-lockdown approach, i.e. “To control access to information as much as possible, sir!” While admirable, this again shows a bit of immaturity. Not really in a bad way, just not quite what I’m looking for. A

much better answer in my view is something along the lines of, “To help the organization succeed. ”This type of response shows that the individual understands that business is there to make money, and that we are there to help them do that. It is this sort of perspective that I think represents the highest level of security understanding—-a realization that security is there for the company and not the other way around.

What’s the difference between a threat, vulnerability, and a risk?

As weak as the CISSP is as a security certification it does teach some good concepts. Knowing basics like risk, vulnerability, threat, exposure, etc. (and being able to differentiate them) is important for a security professional. Ask as many of these as you'd like, but keep in mind that there are a few differing schools on this. Just look for solid answers that are self-consistent.

If you were to start a job as head engineer or CSO at a Fortune 500 company due to the previous guy being fired for incompetence, what would your priorities be? [Imagine you start on day one with no knowledge of the environment]

We don't need a list here; we're looking for the basics. Where is the important data? Who interacts with it? Network diagrams. Visibility touch points. Ingress and egress filtering. Previous vulnerability assessments. What's being logged an audited? Etc. The key is to see that they could quickly prioritize, in just a few seconds, what would be the most important things to learn in an unknown situation.

As a corporate Information Security professional, what's more important to focus on: threats or vulnerabilities?

This one is opinion-based, and we all have opinions. Focus on the quality of the argument put forth rather than whether or not they they chose the same as you, necessarily. My answer to this is that vulnerabilities should usually be the main focus since we in the corporate world usually have little control over the threats.

Another way to take that, however, is to say that the threats (in terms of vectors) will always remain the same, and that the vulnerabilities we are fixing are only the known ones. Therefore we should be applying defense-in-depth based on threat modeling in addition to just keeping ourselves up to date.

Both are true, of course; the key is to hear what they have to say on the matter.

Advanced

If I'm on my laptop, here inside my company, and I have just plugged in my network cable. How many packets must leave my NIC in order to complete a traceroute to twitter.com?

The key here is that they need to factor in all layers: Ethernet, IP, DNS, ICMP/UDP, etc. And they need to consider round-trip times. What you're looking for is a realization that this is the way to approach it, and an attempt to knock it out. A bad answer is the look of WTF on the fact of the interviewee.

How would you build the ultimate botnet?

Answers here can vary widely; you want to see them cover the basics: encryption, DNS rotation, the use of common protocols, obscuring the heartbeat, the mechanism for providing updates, etc. Again, poor answers are things like, "I don't make them; I stop them."

Scenario Role-Play

For special situations you may want to do the ultimate interview question type. This is a role-played scenario, where the candidate is a consultant and you control the environment. I had one of these during an interview and it was quite valuable.

So you tell them, for example, that they've been called in to help a client who's received a call from their ISP stating that one or more computers on their network have been compromised. And

it's their job to fix it. They are now at the client site and are free to talk to you as the client (interviewing them), or to ask you as the controller of the environment, e.g. "I sniff the external connection using tcpdump on port 80. Do I see any connections to IP 8.8.8.8." And you can then say yes or no, etc.
From there they continue to troubleshooting/investigating until they solve the problem or you discontinue the exercise due to frustration or pity.

http://www.danielmiessler.com/study/infosec_interview_questions/

Category I: General Security Concepts / Network Security / OS Security

1) Is there any difference between Information Security and IT Security? If yes, please explain the difference.

Ans- Yes. Information Security and IT Security are both different terms often used interchangeably. IT Security focuses on purely technical controls (like implementing antivirus, firewall, hardening systems etc) while Information Security is more wider term which implies securing "information" as an asset be it in any form. (ex shredding of paper documents to prevent dumpster driving etc). So IT security can be considered as a subset of Information Security.

2) What is the difference between Encoding, Encryption and Hashing?

Ans- At a very high level, all these 3 terms might appear to be similar and people often confuse between them. But each of the technique is distinct and has different use case. The purpose of *encoding* is to transform data so that it can be properly (and safely) consumed by a different type of system, e.g. binary data being sent over email, or viewing special characters on a web page. The goal is **not** to keep information secret, but rather to ensure that it's able to be properly consumed. It does not require a key as the only thing required to decode it is the algorithm that was used to encode it. Examples: ASCII, Unicode, URL Encoding, Base64. The purpose of *encryption* is to transform data in order to keep it secret from others. It uses a key, which is kept secret, in conjunction with the plaintext and the algorithm, in order to perform the encryption operation. Examples: AES, Blowfish, RSA. The purpose of *hashing* is to take arbitrary input and produce a fixed-length string that has the following attributes:

1. The same input will always produce the same output.
2. Multiple disparate inputs should not produce the same output.
3. It should not be possible to go from the output to the input.
4. Any modification of a given input should result in drastic change to the hash.

Examples- MD5, SHA1, SHA2 etc. Hashing is often used in computer forensics to verify integrity of the digital evidence.

3) What is the difference between proxy, firewall, IDS and IPS?

A **proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Firewall is basically meant for network traffic control/filtering mainly at layer-3. It allows/denies packets and connections based on certain pre-defined rules. IDS- Intrusion Detection System is an application which tries to detect intrusion attempts based on attack signature database it has. IPS- Intrusion Prevention System detects the intrusion (like IDS) and goes one step ahead to prevent it as well. It simply drops the packet it thinks suspicious (based on rules)

Examples:

1. proxy – Squid
2. Firewall- IPTables, CISCO Pix, ZoneAlarm
3. IDS- SNORT
4. IPS- IBM Proventia

4) How does asymmetric encryption work?

5) How does SSL work?

6) What is port scanning? What are the countermeasures to prevent it?

7) What is Man in Middle attack? Can it be prevented?

8) What is the difference between false positive and false negative?

9) Explain the term 'Defense in depth'.

10) What do you mean by stateful inspection by a firewall?

11) What is DMZ? Which systems should be placed in DMZ? What are common security precautions for DMZ systems?

12) What is DLP? How does it work?

13) In what scenario, AD authentication should be used?

14) Is SSH completely secured? If not, can it be hardened more?
15) What is Virtualization? What are the security risks in it?
16) What do you mean by 'BYOD' ? Explain security concerns related with it.
17) What are the different layers of OSI model? Can you list 1 vulnerability corresponding to each of the OSI layer?
18) What are honeypots?
19) Tell about any of the major security incident that happened recently.
20) How do you keep yourself updated with latest trends in Information Security?
21) Which OS do you feel is more secure? Linux or Windows?
22) Explain in brief, Multi Factor authentication.
23) Explain in short how Kerberos works.
24) How to harden a Windows Machine?
25) How to harden a Linux Machine?
26) How can you prevent DOS/DDOS attack?
27) What is a 0-Day Vulnerability? Can it be prevented?
28) What is the biggest difference between Windows OS and Linux OS?
29) Can an IDS be used to prevent intrusions? (Ans is yes, ex- SNORT, one of the open source IDS if configured in in-line mode in conjunction with IPTables, it can act as IPS)
30) Explain any type of Wi-Fi Attack and how to prevent it.
31) What is SIEM? Why it is useful?
32) What is rainbow attack? Is there a way to prevent it?
33) Explain the difference between hub, switch and router.
34) What do you mean by reverse shell in Linux?
35) Explain file ACL's (permissions) in Linux. What is the use of sticky bit?
36) What is NAT and PAT? Explain difference between them and how do they work.
37) Comment on security concerns in Cloud Computing.
38) What is the use of 'salt' in reference to passwords? Are there any limitations of using it?
39) What is single sign-on? What are security risks with it?

Category II: VA/PT

1) What is the difference between Vulnerability Assessment and Penetration Testing? Which one needs to be performed first?
2) What are the steps to perform VA/PT?
3) What precautions are required to be taken while performing VA/PT?
4) With whom would you share the findings of VA/PT and how would you convey the risk of the findings effectively so that mitigation can be initiated immediately?
5) What tools do you normally use for VA and PT? Which tool you find the best and why?
6) What all should be included in report of VA/PT assessment?
7) Is it possible to hack into a system without using any tool? If yes, how would you do it? (Manually?)
8) How can you identify whether a remote machine is a Windows Machine or Linux Machine?
9) What is the difference between active and passive information gathering? (give 1 example of each)
10) How does sniffing works? Explain how can you sniff into a network. Can sniffing attack be prevented and how?
11) What would you do if nmap port scans are blocked by network security administrator? How would you gather host information in such case?
12) What are the different components of metasploit? Explain client side exploits/attacks.

Category III: Web Application Security

1) Why is Web Application Security Important?
2) "Making the website HTTPS would make it secure" share your comments on this.
3) What are cookies? What security threat do they pose?
4) What is SQL Injection attack? What are its types?
5) What are the ways to prevent SQL Injection?
6) What is XSS attack? What are its types?
7) What are the ways to prevent XSS attacks?
8) What is CSRF? How to prevent it?
9) What are the top 5 Web Application Vulnerabilities you know?
10) Explain any case wherein you found some critical web application vulnerability and you also provided solution to fix the same.
11) How would you mitigate vulnerabilities in a legacy application where much of code change is not feasible?
12) What tools do you use for performing Web Application security testing?
13) How do you test security for web services?
14) What is the difference between White Box Application Security testing and Blackbox Application Security testing?

15) Do you have hands on knowledge of source code review? Give any example of vulnerability/bug you found during source code review.
16) What standards do you refer for Web Application Security and related vulnerabilities?
17) What are the most important steps you would recommend to secure your new web server?
18) Will L-3 firewall be useful in protecting the web application against common attacks? If yes, then to what extent?
19) What is Directory Listing? What is its impact? How to prevent it?
20) Can you explain any 2 vulnerabilities occurring due to poor session management?
21) Where should be the Web Server and Database server placed in network for optimal security?
21) Is there any risk when conducting Application Security testing on production instance?
22) How would you investigate or trace any security incident which occurred due to exploitation of some vulnerability in your web application?
23) Please explain how would you test a mobile application for security vulnerabilities?
24) Explain about Database Security. What are common controls for securing Databases.
25) How would you convince the developer to fix the vulnerabilities you found in the Web Application?
26) How does HTTP handles state?

Category IV: Risk Management/ Compliance/ Security Frameworks

1) What is Risk Assessment and Risk Management? Are they same?
2) What are the standards available for Risk Management?
3) What are the types of Risks?
4) What are the possible ways to treat the risk?
5) What is the difference between threat, vulnerability , exploit and risk?
5) What is residual risk? Can it be eliminated?
6) What is ISO 27001? Why an organization should adopt it?
7) What is the difference between ISO 27001 and ISO 27002?
8) What is PCI-DSS? Is there any similarity between PCI-DSS and ISO27001?
9) What type of organizations are required to be compliant with PCI-DSS?
10) What is the difference between a standard, policy, procedure?
11) What would you do to make security program / initiative successful in the organization?
12) How would you convince the senior management to invest in certain security initiative?
13) How much would you ideally spend on securing a Windows Server? (This is a very generic question, but would really test whether the candidate is clear with the basics like asset value, impact analysis etc)
14) What is the difference between technical controls and procedural controls? (give 1 example of each)
15) Explain high level steps for initiating and implementing ISO27001.

Category V: Strategic / Scenario Based Questions

1) Please comment: Which one would be more securely built? Open Source software or Commercial/Proprietary software?
2) Whom do you get inspired from in the field of Information Security?
3) How many packets would travel from a laptop if a user initiates a traceroute to facebook.com?
4) Consider a scenario, the network has become extremely slow, there are many escalations coming to service desk, what would you do a as security professional? Do you see a possibility of any security threat in this? How would you face this situation?
5) Suppose business team wants to launch an application or urgent basis, but you know its vulnerable to some critical attacks, what would you do in such case? Should business requirement be given priority or security should be the priority?
6) What are the latest trends in Information Security?
7) Is Internet Banking really safe and secure? What are your views on this?
8) Where do you see yourself (in which role/position) after 3-4 years?
9) Should social networking websites (like facebook) be allowed or blocked? Justify with proper reason.
10) Anonymous hackers are hacking into some critical infrastructure around the world. Can you comment on how would they be doing this?
11) Have you heard about stuxnet? Explain your views on it and how could it have been prevented?

Category VI: Computer Forensics/Laws

1) What do you mean by checksum? What are the popular algorithms for calculating checksums? What is its significance in computer forensics?
2) Describe steganography, its types and how to detect it?
3) What do you mean by file carving?
4) What is meant by bit stream image? Why it is important in forensics?
5) What is swap space? What is its relevance in forensics? What is page file?
6) Explain high level steps for seizing a live computer system.

7) What are the main challenges in computer forensics?
8) What is file shredding?
9) Can data be recovered after shredding is performed?
10) What are the famous tools used in computer forensics?
11) What hardware is necessary for performing computer forensics?
12) What care should be taken while packaging the seized evidence?
13) What is slack space?
14) List few situations wherein lost data cannot be recovered.
15) How would you traced a spoofed email sent from spoofed IP address?

http://sagarr525.wordpress.com/2013/05/08/information-security-interview-questions/

Security Interview Question 1: What is your vision for our security organization?

"The vision thing," as the first President Bush once termed it, is hugely important in selecting a CSO. The company's executives will have their own vision of what a CSO should be and what he should be able to do for the company, and they'll expect you to have one too. They want to know that you have experience with their particular security issues, that you can craft a plan for where security should be in their enterprise—and how you are going to get it there. "In my case, I had a very complete job description written for them and had brainstormed what I thought a CSO should be able to provide them," says Robert Champion, CSO of WGL Holdings, which owns Washington Gas. CSO candidates should try to learn as much as possible about the company and position, and be prepared to discuss ideas and strategies that match an employer's goals.

Security Interview Question 2: How will you fit in with our corporate culture?

The CSO's role at IBM or GE and that same position at Google or Yahoo are worlds apart. Every company that you interview with wants to know whether you can work comfortably with its corporate personality. Before your interview, talk to employees and, if possible, walk the halls. Is this a straitlaced crew, or will you need reserves of flexibility in order to fit in?

When Champion took a walk through the facility after his interview, he compared what he saw with what he had heard during his conversations with executives. "I was able to get a sense of the level of energy, the diversity picture and the material condition of the facilities," he says. "A little attention to detail will also tell you about the security culture. Do people wear their IDs? Are doors propped open? Do strangers get challenged? Can unattended PCs be accessed?" The answers will help you make a career judgment.

Security Interview Question 3: Do you work well with others?

Hopefully the answer is "Yes!" During the interview process, it's likely that you'll meet with a variety of line-of-business executives from HR, legal, finance, IT and so on. Each will want to assess whether you are going to be a partner or a stumbling block to his goals. They're not looking for a pushover (hopefully), but if the company is a collaborative environment, they want to know that you can play in that sandbox. Have examples ready of projects where you have successfully partnered in the past. And talk to these folks about their responsibilities and security concerns in their own language rather than using technical jargon. "They don't have experience in information security, and these executives are tired of talking to security people that can't talk in business terms," says Sharon O'Bryan, former CISO at ABN Amro and now president of O'Bryan Advisory Services.

O'Bryan also suggests that candidates underscore their business fluency by asking non-IT executives questions about business operations during the interview, such as: What business transactions and processes are key profit generators? How has the company used technology risk management capabilities to reduce operational risk management costs?

Security Interview Question 4: What do you think about security convergence and its effect on our company?

xecutives may not use the word convergence, but you can bet they have heard about or have thought about the movement that security is making toward being part of a larger risk management strategy. It is likely that they will try to suss out your perspective and experience in this area at some point during the interview. "You need to be prepared to discuss convergence, what the pros and cons are, and what your vision is for how to get there," says Champion.

Editor's note: For update views on convergence, read 2011's From convergence to Enterprise Risk Management and Risk's rewards: Organizational models for ERM

Security Interview Question 5: How do you sell security to other executives?

Good sales and leadership skills are critically important. After all, what good is all that vision and experience if you can't persuade others to your way of thinking? Veteran security executive Pamela Fusco, an adviser to the Information Systems Security Association, has often been asked to make a sales pitch for a particular business case

during an interview. "Executive management needs to know that you can talk at multiple levels and build a business case," says Fusco.

Security Interview Question 6: How do you sell security to the company at large?

Influencing the average employee also comes with the job, and it's often the greatest challenge for security executives. "You have to demonstrate that you can make people change even when they don't want to," says Robert Garigue, vice president for information integrity and chief security executive for Bell Canada. Candidates should go into an interview with examples of situations in which they were able to change ingrained behaviors and long-established processes to accomplish a security goal.

Security Interview Question 7: Why are you leaving your current job?

This is a question where CSO candidates can sabotage themselves by going negative. It's important to be honest but to also stay positive. Perhaps you are looking for greater opportunities for development, a new career challenge or to launch into a different industry or type of company. Don't use the interview to vent about the inadequacies of your current job.

"I've witnessed a lot of senior security position interviews where the individual was crying over spilled milk," says Kevin Lampeter, chief security and fraud officer with a global financial services firm. "If the conversation is about what everyone did to make their job harder, that tells me that they didn't take ownership. That reflects on a candidate's ability to be collaborative and their interpersonal skills." Airing dirty laundry is also poor judgment, says Lampeter. If a candidate is speaking poorly of his current employer, chances are good he'll do the same thing to the next one.

Security Interview Question 8: Are you willing to be accountable for security?

This question digs into your knowledge about government regulations that apply to the prospective employer. A candidate needs to be conversant with any regulations that affect the company he's interviewing with, and must show he can integrate business requirements into an overall security program and organization. "They take for granted that you understand all the baseline physical and IT security stuff," says Champion. "They want to know: [Do] you understand their compliance environment and Sarbanes-Oxley? Can you interpret aSAS 70 report from an IT vendor? How will you keep them out of hot water with regulators, auditors and shareholders?"

Security Interview Question 9: Are you a risk-taker?

Security executives are often walking a fine line when they talk about risk with business owners. Business leaders want a CSO who is a risk-taker because they want to do more, do it faster, and they don't want a security executive who constantly says no. In the interview you have to demonstrate that you have a balanced approach to risk and that you are willing to explore ways that the company can take on more risk if that's what it wants to do. "We've all got great examples about how we said no," says Garigue. "What we need are examples of how we said 'yes, take the risk,' but in a controlled way."

Security Interview Question 10: What does this role mean to you?

Once you've gotten through some of the more technical and strategic questions, it's likely that at least one interviewer will throw you an open-ended question like this one. This is your chance to talk about what makes you unique. When Baird was asked this question at United Rentals, it was a welcome opportunity to lay out his perspective. "I explained what I could bring to the table, how I would fit in, and I was candid about the type of organization that I wanted to build. It was a chance to then turn the question back to them and ask if that was the kind of security organization they wanted in their company," he says.

One final thought: CSOs are still the new kids on the block. So don't get hung up on giving the "right" answer or projecting yourself as a traditional CSO, because there is no such thing. "Remember," says Garigue, "the different organizations, problems and laws that you have had to work with have evolved you into the person you are today."

http://www.csoonline.com/article/220900/10-tough-security-interview-questions-and-how-to-answer-them?page=4