NewCISOJob

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy, and today we're gonna talk about are you ready to win your first CISO gig? This is an opportunity to learn some tips and tricks about how to navigate the hiring process if you're looking for your first CISO job.

[00:00:33] **G Mark Hardy:** Or maybe if you're looking to step up a level to the next CISO job, in any case, please listen in, I think you'll enjoy this. And as always, make sure you're following us on LinkedIn cuz you get so much more than our episodes. And please make sure that you give us a thumbs up somewhere so other people can find us as well.

[00:00:51] **G Mark Hardy:** On our CISO Trade Craft podcast, we talk a lot about the role of a CISO, and one of the things we haven't spent much time on is how to actually win a CISO [00:01:00] position. So let's take a look at the process of what that looks like and how you need to perform to bring home the bacon. The first thing to know is that not all CISO jobs are the same.

[00:01:10] **G Mark Hardy:** There can be a huge difference in roles. Here are just a few examples. The first role we'll look at is the startup CISO. The CISO role is being created in a new startup, and so you're the first cyber employee. Wow. While this means that you'll generally spend your time building up the organization and explaining why cyber processes are needed, unfortunately your peers might see cyber as slowing down the rapid innovation and expansion of the company.

[00:01:34] **G Mark Hardy:** And you'll fight constant battles for funding with both, for tools and as well as for any additional staff. The second type of CISO role is a segment CISO role, which can be commonly thought of as a business information security officer or BISO role. In the segment CISO role, you'll have a big focus on product security and cyber policy interpretation and vulnerability management for a large division of a company, however, you don't actually [00:02:00] oversee the security operations center.

[00:02:02] **G Mark Hardy:** Or the engineering efforts, and thus, your ability to control and determine security relevant decisions such as which antivirus or

DLP, or firewall, or WAF or SIEM the organization should choose is extremely limited. However, this can be a great opportunity to learn how to influence and persuade others when you do not have management authority.

[00:02:23] **G Mark Hardy:** The third CISO role is actually a split CISO role. For example, large banks may split the CISO role between one, which is technical and one which is not technical, and this is very common in the financial sector where they leverage a three lines of defense model.

[00:02:37] **G Mark Hardy:** The first line is focused on management of the cyber defenses. The second line is focused on risk management and compliance, and the third line is internal audit. So the biggest problem is the first and second line. CISOs need to be on the same page with what they're telling their executives. For example, if the first line CISO says, we need to spend 2 million to overhaul the SOC. And the [00:03:00] second line CISO says, well instead, we need to spend those 2 million on increased maturity. With SOC two compliance, the executive team gets mixed messages and that confusion. Will likely push back a decision on where to fund, when to fund, what to fund. It's creating a lose lose situation for both CISOs. Now that being said, if you can get on the same page, having two different cyber leaders informing executives how to improve cybersecurity makes for a great approach to changing the organization, particularly if you're able to go ahead and deliver a unified message.

[00:03:35] **G Mark Hardy:** And the fourth type of CISO role is that of a traditional CISO that owns the show, and that person has management authority over the soc, over grc, over security, engineering, pretty much all the security functions. There isn't the second line of cyber defense per se. Remember, that's the risk management and compliance function.

[00:03:53] **G Mark Hardy:** But now the CISO owns all that, but there is an audit function and when you're in this CISO role, you have full [00:04:00] accountability for when things go well or go badly, and hopefully you're considered an officer of the company, which will grant director and officer's insurance because this role can come with a great deal of potential professional liability.

[00:04:13] **G Mark Hardy:** Okay, so now that we've seen four different types of CISO roles, Let's understand that there are tiers of CISO level roles, which are generally based on pay scales and the size of the organization. For example, most large Fortune 100 companies will not hire a first time CISO. They want someone with proven CISO experience.

[00:04:32] **G Mark Hardy:** These Fortune 100 companies can also pay the million dollar salaries and bonuses to attract top tier talent. Now, if you're a cybersecurity senior director, managing a team of 10, making 200 k saying to yourself, well, my dream is to become a CISO at a Fortune 100 company, then consider the following path.

[00:04:52] **G Mark Hardy:** Take a CISO role at a small company with an entry level salary. Could be a couple hundred grand, could be three to 400 K, where you [00:05:00] oversee a cyber department of 25 people. Now here you get more time working with executives and getting practice on how to drive the entire cyber strategy for the company.

[00:05:09] **G Mark Hardy:** Don't get too hung up on compensation at this point. There are government opportunities, there are nonprofit opportunities that are not gonna be able to pay these top level salaries, but can give you some spectacular experience and some great resume credentials that are gonna allow you to go ahead and move up to a higher level.

[00:05:28] **G Mark Hardy:** So be careful about chasing the dollars right out of the door. You might find out that doing so is a little bit frustrating because there are those who have already put in the time and have built the credentials and have been willing to sacrifice a little bit of the short term income for the opportunity to make more in the long run.

[00:05:46] **G Mark Hardy:** Now, after a few years of doing your small company bit or nonprofit or government, you decide you wanna move to a medium size corporation. Now your salary doubles. Maybe you can make as much as 600 grand with maybe even up to 800 grand when you've got [00:06:00] bonuses and incentives in there. Now the cyber organization you oversee is now 50 to a hundred people, which means.

[00:06:06] **G Mark Hardy:** You've got twice as many activities to supervise. And since the organization is larger, there's a huge focus on compliance and controls. The company has mentally shifted from just enough cyber to survive being hacked to the mindset of how can we win against the larger businesses who are our competition?

[00:06:23] **G Mark Hardy:** And this generally means you need to pass a SOC two, type two type of an audit, generate that report, or have an ISO 27001 certification. Midsize companies also need to spend more time on their best employees, since they're generally at the most risk of being poached by companies that can pay more and sometimes pay a lot more.

[00:06:43] **G Mark Hardy:** And finally, after being a CISO, a medium sized company for a few years, you get called by an executive search firm who's looking to fill a large company, CISO role. The large company wants you to lead the cyber organization of 200 plus folks and offers you a package of one and a half million [00:07:00] dollars to run the show.

[00:07:01] **G Mark Hardy:** Wow. Now, that's kind of aspirational and some people get there. Personally, I'm not there, and I'm probably not on that track, but have enough professional associates have been able to be successful that I can credibly share these insights with you. Now different companies recruit differently, but often use similar approaches based on company size.

[00:07:25] **G Mark Hardy:** Small companies post their CISA roles on LinkedIn. Medium size companies will use both HR recruiters and executive search companies to find qualified applicants. Large companies will a hundred percent outsource their executive recruiting to one or more executive search firms or promote from within. Now, if you're looking for a large company CISO role on LinkedIn, I think you're in the wrong place.

[00:07:50] **G Mark Hardy:** Now, let's say your friend works at a healthcare company and tells you that their CISO's just left the company. They're now looking for a new CISO, and your friend is gonna recommend you as the next CISO to the [00:08:00] recruiter? Well, first of all, that's awesome. This is exactly the type of personal network that you wanna be building.

[00:08:07] **G Mark Hardy:** Now you need to focus on winning that role. So let's go through the process. The first thing that someone will look at is your resume and your LinkedIn profile. So you need to make sure those look like an executive. Let's start with an example of, well, what not to do. You list all the technologies that you've learned over the last 15 or 20 years on your resume.

[00:08:28] **G Mark Hardy:** The resume contains a lot about the activities of performing risk assessments, finding vulnerabilities during pentests, and performing incident response. Anyone, any type of recruiter who reads your resume gets a feeling that this applicant reads kinda like, well, a computer or programmer or technical person.

[00:08:46] **G Mark Hardy:** They can tell you're smart. They can tell you're technical, but they can't tell you if you're any good at your soft skills. And additionally, since your resume focused on all the busy work of activities, recruiters don't actually know if you are effective. [00:09:00] And if you could go ahead and manage teams to make that happen.

[00:09:03] **G Mark Hardy:** Now, this could be a big problem if your resume also shows a pattern of job hopping every two years or less. Recruiters may be wondering, were you fired? Were you ineffective? Or were you just chasing the money? Basically, all bad signs that signal you're an unnecessary risk that many recruiters and hiring managers, they tend to avoid.

[00:09:22] **G Mark Hardy:** Okay, so if you don't wanna focus your resume on only technical expertise and activities, well, what should you write about? Your resume should focus on three things, technical skills. Soft skills and executive leadership skills. Now, one example of how you might accomplish this is by placing an executive summary section at the top of your resume that says something like the following.

[00:09:46] **G Mark Hardy:** The first point to make is you enable and safeguard the business. You're considered an expert in application security, product security, cloud security, DevOps, and desktop security. You led three organizations through the [00:10:00] successful adoption of Amazon Web Services as well as the application of security controls.

[00:10:05] **G Mark Hardy:** This is technical enough for an HR CFO representative to understand what you did and the impact you made without the excessive detail of tool names like Fortify or Web Inspector Qualys or Jenkins, which really kind of mean nothing to a recruiter.

[00:10:19] **G Mark Hardy:** The second point to make is that you are a great communicator who can connect, convey, persuade and influence. You communicate effectively with both technical and non-technical audiences, and that's key. Over the last two years, you led the vulnerability management program to understand what posed the biggest risk to the organization. By leveraging gamification techniques, you drastically change the culture and reduced the vulnerabilities and critical SOX opportunities.

[00:10:48] **G Mark Hardy:** By leveraging gamification techniques, you drastically change the culture and reduce the vulnerabilities in critical SOX applications by 90%. And this occurred because you led the identification of the [00:11:00] technical vulnerabilities that were most likely to be impactful to the company. And by repeatingly working with the CIO and direct reports changes occurred.

[00:11:08] **G Mark Hardy:** It kept the executive team informed of the various progresses, and you met key objectives throughout the year. Now the last point to make into the executive summary section is that you are a great executive

leader who inspires others. You focus on the people within your organization by building talent pipelines to retain employees.

[00:11:31] **G Mark Hardy:** You champion diversity initiatives through employee resource groups and found novel ways to attract new talent, for example. Be sure you notice that the third party vendor review process seemed to require high attention to detail, and the process also appeared to be very repetitive. Your team members were not taking to the task and nobody really wanted to do it well.

[00:11:51] **G Mark Hardy:** So you partnered with a company that focuses on providing neurodiverse talent and this result in the cyber organization bringing on talent that had incredible strengths and [00:12:00] detail-oriented roles with repetitive tasking. Your current organization built a competitive strength. From attracting new talent that most organizations have avoided, your partnership with the Neurodiverse community created incredible company loyalty and promoted a very positive brand within the community.

[00:12:18] **G Mark Hardy:** Now once recruiters get past the executive summary section of your resume, it's time to highlight your job experiences. Remember, don't get bogged down in just listing all the activities that you performed and the technologies you know, tell a story using the STAR method. STAR stands for Situation, Task, Action, and Result.

[00:12:40] **G Mark Hardy:** For example, as the head of the incident response team, I was responsible for leading 20 analysts to perform 24 x 7 coverage of security incidents across the company. And this meant that I had to understand how log activity was occurring from databases, desktops, and server applications. I also knew to create an optimized process where logs [00:13:00] could be filtered to create cyber attack alerts on risky activities. And therefore, I led the team to compare logs against the MITRE attack framework, which identifies the most probable attack methods used by bad actors to attack a target. We created custom alerts in our security information and event management tools, our SIEM, as well as automated responses in security orchestration and automated response platform.

[00:13:21] **G Mark Hardy:** That's a SOAR now again, when you mention those, spell 'em. Put the acronym and parenthesis right after it, just in case reader's not familiar with it. Okay, so let's finish. And as a result of these focused alerts and automated responses, we reduced the volume of data needed. For our SOC to process this resulted in a million dollars in cost savings, quicker

response times to alerts, and huge improvements in employee morale within the security operations center.

[00:13:48] **G Mark Hardy:** Analysts went from chasing false positives 80% of the time to less than 20% of the time. And these changes to organization result in stopping two major cyber attacks by ransom operators. Now [00:14:00] how did that sound? Little bit focus of what you're doing. You go. You look at the situation, we talked about the task, the actions we took, and the result.

[00:14:10] **G Mark Hardy:** If you can show positive results because of your. Leadership. Because of your direction, because of your actions, you've got a much stronger story to tell. See if any recruiter reads that resume, they'll say, well, look what this person is done. It looks pretty awesome and this is the right type of talent that we want at our company.

[00:14:31] **G Mark Hardy:** Now, you don't need to list all the technologies and boring activities. Remember, you are no longer applying for a technical role. You are applying for an executive role. And you're showing recruiting and hiring managers how you create impact, which is what they want. Once you start using the STAR format to describe your career accomplishments across multiple jobs, you need to ensure your resume shows you as a well rounded CISO.

[00:14:56] **G Mark Hardy:** Now, this is important because if people only think of you as [00:15:00] the incident response CISO, and this new role needs to lead an audit and compliance team as well, then you're gonna be deemed unqualified. So here we've got a couple recommendations. First, look at the job description. Job descriptions contain the checklist of hiring requirements that you need to display in your resume, and make sure your resume can speak to most of those requirements.

[00:15:22] **G Mark Hardy:** Be careful about painting into the corners. If there's 20 things on that list and you list exactly 20 things in your resume, no more, no less, you're just sort of parroting back the job description. Remember what the purpose of this resume is to do. It's to get you that interview. You wanna have 16, 17 of the 20.

[00:15:40] **G Mark Hardy:** That's a good hit, and then you can talk about the difference on the rest of 'em. So be very careful about trying to be a little bit too cutesy in terms of how you put your information together. But also there's an absolute strong case to customizing your CV to a particular opportunity. If you

have the same thing you throw at [00:16:00] everybody, it may or may not work very.

[00:16:02] **G Mark Hardy:** Now. Secondly, you find it's helpful to make one resume that can be applicable for most CISO post. Now if you wanna do that, okay, then you can apply for 20 different jobs with minimal effort. But again, if I'm looking for somebody who's gonna do a CISO role, do I want somebody who is good at minimum possible effort?

[00:16:20] **G Mark Hardy:** Maybe not, but if you wanna go that way, at least to go ahead and hopefully that it breaks the ice and get you started. You can go ahead and look at the CISO Mind map from Rafeeq Rehman you may remember him from episode number 86. We brought him on the podcast to talk about the CISO mind map, and you can also found a large number of activities that you need to demonstrate to be a well-rounded CISO.

[00:16:41] **G Mark Hardy:** We've taken his mind map and summarized them to create the top 10 knowledge domains of being a CISO. And if you're looking to identify the top 10 CISO domains, please check out CISO Tradecraft episodes number 59 and 60, where we provide a lot more detail. All right. Once you've got your resume and working [00:17:00] order, then you need to know if it's effective.

[00:17:02] **G Mark Hardy:** The way you know it's effective is by the results. Let's say you applied at 20 CISO jobs on LinkedIn, and if you get asked to meet with the HR representative in three to five of those organizations, then. You know your resume's working. If you get asked to meet six or more times and you know your resume's working really well.

[00:17:19] **G Mark Hardy:** Now, if you don't get at least three interviews, well, something's wrong with your resume. It's either poorly written or the job level you're competing for, or too far out of your carbon job experiences. Remember, if you haven't been a CISO before, it really doesn't matter how well your resume's written when you apply to be a Fortune 100 CISO role.

[00:17:37] **G Mark Hardy:** The sad truth is you're just not gonna make the cut. Okay, so let's say we've got some good news and your resume found its way to recruiter who read it, asked you to make an appointment for phone call or Zoom meeting. What should you focus on during that 30 minute conversation? Your focus should be on one thing, getting to the next step in the recruiting process.

[00:17:57] **G Mark Hardy:** That's it. Recruiters [00:18:00] wanna tell you about the culture of the company. They wanna see if you'll be a good fit within it. They'll also be on lookout to see if you have too much of an ego, and to differentiate yourself from other candidates who might be all absorbed into themselves. You need to emphasize that you're humble, collaborative. You can partner to change an organization at the right place.

[00:18:19] **G Mark Hardy:** See, nobody wants a seeso to come in like a bull in a China shop. Now, I dunno, if you're a ceo, it's a different story. But imagine you get a question that says, what would you do first if you took the role as a CISO? If you respond from a technical point of view and say, well, I'm gonna look at antivirus and secure the WAF and perform pentest, then you'll fail the interview.

[00:18:40] **G Mark Hardy:** You must focus on the human experience. So try to respond with something like the following. I'm gonna meet with my boss, my direct employees, and various peers across the organization. I'm gonna ask questions from them to understand what's working well, what isn't working well, and what things a cyber organization should be doing to [00:19:00] improve the business.

[00:19:01] **G Mark Hardy:** Once I hear repeated themes, I need to understand why certain decisions have been made or haven't been made. There's important history to understand why certain decisions failed or didn't go smoothly, and once I know those, I can prioritize opportunities based on a level of effort versus the impact to improve cybersecurity.

[00:19:19] **G Mark Hardy:** I'll present my findings within the first 90 days of arrival as a new cyber strategy to the executive leadership team pending buy-in. Of course, I'll work to create a program plan that outlines when these activities can be accomplished and go from there. Now, if you compare these two answers, the first one's about technical skills in your ego.

[00:19:38] **G Mark Hardy:** Remember, I gotta look at the antivirus, secure, the waff, et cetera. I can find all the security problems, fix them with just technology. No, that's not what you're looking for. The second answer is about partnership, influence, and socialization to begin the journey. The second answer gets you past the HR recruiter gatekeeper, and towards an interview with the hiring [00:20:00] manager.

[00:20:01] **G Mark Hardy:** The other question you can likely expect to receive is something like, tell me a little bit about yourself and why you're applying for

this role. Now they don't want a life story. They want a concise recap of your resume. So give 'em the Cliff notes version. Well, I earned a computer science degree and went to work at my first job at the XYZ Company, and here we learn how to be an IT security analyst by performing incident response and troubleshooting firewalls and laptops.

[00:20:28] **G Mark Hardy:** Then took a job as a GRC specialist where I helped audit various organizations to understand their cybersecurity controls and practice. Got to learn a lot about compliance. And ensure the organization was adhering to it. I knew I wanted do cybersecurity leadership for the rest of my career, so I completed an MBA that allowed me to understand the mindset of being a business executive.

[00:20:46] **G Mark Hardy:** And after graduation, I took a management job as the leader of the DevSecOps organization. I led a team of 15 people that provided all the software tools to developers, it was pretty awesome. And we hosted 10 different tools that allowed [00:21:00] nearly 10,000 developers to build software cheaper, faster, better than ever before.

[00:21:05] **G Mark Hardy:** And finally, I took a role as a manager over 10 business information security officers. I got to partner with executives and transform cybersecurity within the organization. We reduced vulnerabilities by 90% while also launching major IT programs that were secure and they greatly benefited the company. It was a lot of fun to help this organization. I've been really looking forward to another opportunity to do something similar and I guess that's what caught my eye about this role when I saw the job description.

[00:21:34] **G Mark Hardy:** Remember to keep your answers short and succinct. That might have actually been a little bit too long. See, the recruiter may have 20 questions to ask you in a 30 minute call, so it's best to keep your answers to less than one or maybe two minutes each. If you spend 10 minutes responding to the initial question about your history, then.

[00:21:50] **G Mark Hardy:** HR won't be able to complete their interview score sheet, and essentially HR may conclude that you're long winded and likely have to reject you as a candidate. So be clear, be concise, [00:22:00] and be ready to move on to the next question. Now at the end of the recruiter interview, you'll get asked, what questions do you have for us?

[00:22:08] **G Mark Hardy:** Remember, you're talking to a recruiter, not the cio. The recruiter is judging you based on the questions you asked since it shows how socially astute you are. So try asking a couple questions like this.

[00:22:21] **G Mark Hardy:** Can you tell me a little bit about the hiring manager's leadership style and the culture that seems to work best here at this organization?

[00:22:28] **G Mark Hardy:** And what do you like best about working here at this organization?

[00:22:32] **G Mark Hardy:** See the first question's focused on culture and leadership. You show that you're interested in how the company behaves, not just what the job entails, and that should create a positive vibe for the recruiter. Now, the second question allows you to continue positive feelings since you're talking about. What the other person likes best, and this can bring up even more positive vibes, and the end result is you've created two questions that result in positive feelings within the recruiter's mind, and now the recruiter's singing that maybe you're quite likable and you're [00:23:00] having a great conversation and this might work out.

[00:23:03] **G Mark Hardy:** Now the last question you need to ask about is the next step to win the job. Say something like, I've really enjoyed learning from you about this company and it's wonderful culture, and it seems like a place I'd love to be a part of. Can you tell me more about the hiring process and what the next steps are that need to happen?

[00:23:20] **G Mark Hardy:** See, once again, you're asking the recruiter about something that they should know a lot about. You're also informing them if you're interested to continue the interview process and after the recruiter informs you of the next steps, simply say That makes a lot of sense. Thank you. Will you be recommending me to talk to the next person for an interview?

[00:23:37] **G Mark Hardy:** It's simple, it's direct, and you'll generally get the feedback to know how well you did. Now let's keep going. Soon you get fantastic news because recruiter enjoyed the conversation, is setting up an interview with the hiring manager and now you get a chance to actually learn about the role from your future boss.

[00:23:54] **G Mark Hardy:** The boss tells you about the role and what they're trying to do within the company. They'll ask you about your background and you [00:24:00] can provide a similar answer to what you told a recruiter. The hiring manager asks if you're technical and can talk to engineers and get their respect. And the answer to that question is clearly yes, and you need to give an example to validate, but you can be technical.

[00:24:12] **G Mark Hardy:** For example, you might say that you, on your hobby timing, write Python code to script out some security ideas that you wanna implement, but you don't have a vendor tool to do that for you yet. Now don't fib here though, I mean, getting caught in a lie is a great way to terminate your hiring process on the spot.

[00:24:26] **G Mark Hardy:** You also need to highlight how you can communicate with non-technical executives. For example, if the hiring manager asks about your approach to risk management, you might say, I think there's a lot of risk management. It's about making informed decisions. And one thing I like to do is meet with the CFO.

[00:24:42] **G Mark Hardy:** I like to ask for spending level authorities within the company to understand them because this allows me to learn things like a manager can approve a $10,000 purchase. A director can approve a hundred thousand dollars purchase, and VP can approve a million dollar purchase. So what? Because once I understand the [00:25:00] currently accepted spending authorities, I can then determine risk tolerance and who has the authority to make certain decisions.

[00:25:06] **G Mark Hardy:** Think about it. If a director can only approve a hundred thousand dollars in new software, then a director should only be able to accept software risk of equivalent value. I look at risk assessments to determine the likelihood and impact of perceived risks and create estimates in terms of dollars. I like to talk to executives about what is a benefit to the business with this software and what is the consequence in terms of risk, and this allows a business leadership to make risk informed decisions going forward.

[00:25:32] **G Mark Hardy:** I learned a long time ago if I only tell the business, no, they'll just go around me. However, if I provide them with all the facts, And allow them to make informed business decisions, they generally arrive at the right outcome. So I make sure risk management decisions are formally documented and approved at the appropriate levels to enable profitable growth for the business while being secure.

[00:25:52] **G Mark Hardy:** Hmm. Okay. So now the hiring manager knows your technical and have the ability to work with executives and influence the [00:26:00] organization. The hiring manager asks what questions you have for me. Now here's some great questions to ask a hiring manager.

[00:26:07] **G Mark Hardy:** How has this role changed over the last year? What are the biggest changes that you see coming to the role in the next 12 months?

[00:26:14] **G Mark Hardy:** How about, can you tell me about the current team size of the organization and the roles and responsibilities I would have in this role? And are there any plans for the team to increase in size or scope within the next six to 12 months?

[00:26:27] **G Mark Hardy:** Can you tell me a bit more about reporting responsibilities? For example, who reports to the board of directors or signs SEC documents about the status of the cybersecurity program?

[00:26:39] **G Mark Hardy:** Can you tell me about the organizational structure of the IT department? What's the reporting structure of this role with respect to the cio and is there a second line cyber risk organization in place?

[00:26:51] **G Mark Hardy:** What do you envision as the hardest part of my new job.

[00:26:56] **G Mark Hardy:** Imagine yourself a year in the future, and you say to [00:27:00] yourself, wow, I'm so glad we hired this person. What accomplishments would you have seen from this role that would've made it success?

[00:27:08] **G Mark Hardy:** All right. Now, these aren't exact questions. I don't think you want to just use this as a script, but they allow you to learn about the role and if the role is actually positioned for success. Remember, if they can't tell you what success looks like in a year from now, then you probably can't achieve it.

[00:27:23] **G Mark Hardy:** And also, if you don't have the resources or reporting structure that you feel is necessary to achieve success, Then you should avoid taking the job. I have seen sometimes where the CISO job is really the chief internal scapegoat officer and it comes with responsibility without authority, and it puts you in a situation where you don't get the opportunity to make the correct influences to make things successful.

[00:27:47] **G Mark Hardy:** Be on the lookout for that. Not everybody is setting you up for success. I have turned down job opportunities because it just didn't feel right. And later on find out that that spidey sense was [00:28:00] actually correct. So if you could get a feel that something's just not right, take a little bit of extra time or poke around a little bit, or be careful about moving your family and your career in a different location if it turns out that this is not gonna work out.

[00:28:16] **G Mark Hardy:** Now, we've talked about a lot of things and the big point to remember is you need to be agile. You need to focus on how to accomplish the next step and to move forward and then ask the questions that the person on the other side of the table can answer. You wanna create an atmosphere where the questions you ask make you viewed in a positive light.

[00:28:36] **G Mark Hardy:** And if you do these things and highlight your skills in a way that shows you as a collaborative and humble executive, then you've created the best opportunity to win your first CISO role. We'll have to continue this episode with part two at a later time that focuses on negotiating the best hiring package and things to watch out for an employment contract.

[00:28:54] **G Mark Hardy:** So be sure to be subscribed to the CISO Tradecraft Podcast, and that way you can get all the future episodes [00:29:00] as soon as they're produced. So thanks again for listening to CISO Tradecraft, and we're so grateful to have you as our listeners. And if you learn something today, please leave us a review on your podcast platform, hopefully five stars, and drop us a comment on LinkedIn.

[00:29:13] **G Mark Hardy:** We'd love to know what you like best about this episode. We've given you any advice. It's helped you land a job and receive your feedback on how we can approve the show. And if you prefer, you can also leave us a comment on our website at CISOtradecraft.com. This is your host, G Mark Hardy. Thanks again for listening and stay safe out there.