#202 - Cybersecurity Crisis: Are We Failing the Next Generation?

[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. I'm your host, G Mark Hardy, and today we're going to be diving into a critical issue facing our industry, how we might be failing our upcoming generation of cybersecurity professionals.

And so we're going to take a look today at some common misconceptions, some challenges in our workplace, and of course, what can we do about it? So let's start by looking at some of the myths and delusions that are out there in the cybersecurity industry today. The first one that I think a lot of us have been talking about is the talent shortage myth.

There's a narrative out there that says we have insurmountable talent shortage. There's hundreds of thousands of jobs in cybersecurity that go unfilled. [00:01:00] All you have to do is go out there, get a degree in IT or cybersecurity, and companies are just going to line up and they're going to offer you all of these high paying positions, and you're going to have to decide just like a, Top draft pick out of a sports, industry, which job do you want?

yeah, and of course you got bootcamps and cyber certification courses. It'll cost you an arm and a leg, but the point is they're going to give you a fast track to a lucrative career. Here's where it breaks down. As a CISO, and other CISOs, we're getting pitches from MSSPs, Managed Security Service Providers, and they say, hey, we'll outsource a lot of these security functions for you.

And it's the tempting offer because it's a whole lot easier to just hand something over to somebody on a contract basis that A has the resources, B has a track record, and then I don't have to worry about hiring and retaining and trying to do all the other stuff about trying to get people on staff, particularly if the requirement is not a [00:02:00] 40, 50 hour a week job.

And so therefore, MSSP seemed to be a good alternative, except for positions where I absolutely got to have somebody here. Then I have MDR, Managed Detection Response Teams. They're everywhere. And it's suggesting, again,

there's a shift toward outsourcing operations. And so that leads us to an interesting observation.

I believe that the real talent gap is not at the entry level, it's at the mid career bracket, and the challenge is going to try to find high quality candidates for middle management roles who've got up to date technical skills in areas like cloud testing or cloud security, pen testing, even AI now, while meeting budget constraints in a lot of environments where companies are starting to tighten up.

We've had a heck of a run in the stock market the last year or so. We'll see what happens after the election. Of course, that's usually when reckoning occurs. But the reality is that a lot of companies aren't flush with cash [00:03:00] for new hires. So let's break this down a little bit. This is the trend that I mentioned, which is outsourcing and cyber security, the reducing the demand for in house cybersecurity professionals, particularly entry level, because a lot of these basic security functions are going to be handled by an external provider.

And quite honestly, they're going to be able to do so for probably a more cost effective basis. You don't have to spend the time and the money and the effort training them to do it. They're already ready and up and going. Secondly, while you've got all these entry level positions out there, again, the scarcity is people who can bridge the gap between a technical expertise and management skills.

And this is not entry level. This requires technical knowledge, developing over a period of time, learning how to work management projects. Deliver on time, on budget, working with different teams, being able to produce reports correctly, ultimately growing into leadership capabilities, [00:04:00] and then your business acumen.

And these combinations, they take years to develop. I came to go to MBA. When I went to my business school, I got my MBA. Didn't instantly make me an expert in organizational behavior and things such as that. I had the fundamentals. But I had to go ahead and build past that point. And that takes time. Also the current economic environment, I've seen people on LinkedIn getting laid off and they've been around for a while.

And so all of a sudden you've got experienced professionals, people with defendable resumes, people. Being up there on the job market and they've had financial pressures and they will take lower level positions to get the cash flow and that's going to squeeze out a new graduate. for the same amount of money, would you want somebody with zero years experience or five or six?

And it's not like that's damaged goods. It's just the nature of the market. And [00:05:00] then fourth, it's important to recognize that educational institutions, certification programs, let's face it, they have their own financial incentives. And so they will benefit by promoting the idea of a high demand and guaranteed employment.

And even if it doesn't align with current market reality. So you've got to be careful that you're not getting sold a bill of goods here. And, Lastly, think about the job market is very regional. So in areas like Silicon Valley, perhaps in the New York metro area, there may be some great opportunities up there.

go to other areas. You may not see so much opportunity. And unless you're willing to pull stakes and go someplace, you might find out that you're not going to be able to be very successful in finding an entry level cybersecurity job. What are things that we can do to fix this? Better collaboration between industry.

in the educational programs to ensure that the curricula will align with real world needs. When I had served with an advisory board, [00:06:00] I spent nine years in the national cyber watch, and we looked at the NISTISSI 4011, 4013 curricula and got two year colleges and four year universities to align their curriculum so that if you did all the courses that you're supposed to do here, you could then roll onto a four year university and not have to retake anything.

And they were designed to go ahead and match what the requirements are that are out there. The hard part is of course, that things change so quickly. And if you have an industry where the job requirements are changing every 18 to 24 months, because, half of what you know about security is going to be obsolete in 18 months, then it's a little bit difficult to make that happen.

We also have to provide our aspiring cybersecurity professionals with all the tools. Honest, data driven insights at a job market, in terms of things such as which specializations are going to be most valuable and even regional areas where they're going to have to go ahead and possibly up and move if you want to go do this stuff.

We need great [00:07:00] internships and apprenticeship programs, and that's a great gap filler when somebody is perhaps in their sophomore or junior year. Going to the next level to say, Hey, come work this summer with the company. And I had hired interns before. I remember talking to one intern, she was from Cornell, and she said, what do you, I said, what?

What do interns get paid? I said, A lot of companies won't pay interns anything. It's a privilege to work here. And I said, what can you get? And he said, if you're lucky, you will. They're like 15 bucks. Whatever it was, I said, I'll give you whatever the max is and I'll go ahead and pay the taxes beyond that.

I want to make sure that you can focus on this job. If you're delivering value because I've created this apprenticeship program correctly, great. If I did the internship program wrong, I overpaid. I didn't overpay hundreds of thousands of dollars either. So if you're thinking about doing interns and things like that, don't get cheap.

Don't go ahead and make these people walk away saying, man, I worked my tail off, but I'm still having to scrape together some money at night to get something to eat. [00:08:00] Pay him a decent wage. And then also there are other people in the IT career fields who can transition to cybersecurity and that expertise they've already built The corporate knowledge, the awareness of how businesses work is going to be very valuable for them in a mid career role and they may be able to fill those gaps.

So that's the first illusion out there that we have, which is, hey, there's all this talent shortage out there. The reality is, it's very specific. What's next? That education will provide job ready skills. See, if all you got to do is get a four year college degree, you open up that matchbook cover and said, would you like to be a long haul trucker?

Or you can open up the matchbook cover and said, hey, you want to be a cybersecurity professional? And boom, you get the degree or you get the cert and instantly you walk into a job. It's not reality. And so what happens is that in the educational world, we find that there's some gaps. Now, I had served as adjunct professor in doing cybersecurity graduate work stuff. And what I found, [00:09:00] and this is not a criticism, it's an observation, is that the edu world has relatively Ossified processes for being able to get curriculum updated and changed. You have to go through all these boards, reviews, and things like that. And it takes a long time to get things current.

Why? Because traditionally things didn't change. Chemistry hasn't changed in 300 years. Mathematics hasn't changed, at least some, unless you're talking about the absolutely new stuff, in a few years. Other than things like quantum physics, you go back to the classic physics, it hasn't changed. So you don't have to do a whole lot.

But in cybersecurity, including IT, things change very rapidly. And so what happens then is that if you have to deal with a three to five year cycle of being able to update your material, Then what happens is, as an academic program, you're going to focus on theoretical concepts, and historical case studies, and things that aren't [00:10:00] going to change a whole lot, and as a result, they are not going to reflect the rapidly evolving landscape of current cybersecurity threats and practices.

Also, and here's a key thing, a lot of universities don't assign a budget or resources to provide the students with the hands on experience using enterprise grade security tools. Instead, they're going to rely on free or open source alternatives, which are great for learning the concepts, but it doesn't prepare you for real life.

When someone sits down in a console and said, there, there's Splunk. Oh, I've heard about it. Have you ever spent time on it? No, but you've got a cybersecurity degree and it says you graduated with an A and you don't even know how to operate these tools. And that's also true in. Many organizations beyond just academia.

If you're looking at certification bodies, they're going to do the best they can to squeeze out the most profit, which means they're going to try to go ahead and not buy high end commercial stuff for people to train on. Mostly because the licenses aren't designed to do that. But secondly, if you've only got [00:11:00] somebody here for a few days or weeks, then out the back end, why spend money on it?

And so that's a gap that's out there and you're not prepared effectively. Exercises in academia really don't have the complexity or the urgency of a real world security. You might do great solving a puzzle or a problem that's set out in a textbook and you go through and you click it and you write it down and you have time to work on it, but that's not real.

The reality is you've got ambiguity in there and time pressure and security happens to have both those characteristics. We don't train very well for that. And a lot of educational programs. In cybersecurity, don't emphasize soft skills like communications, teamwork, business acumen. These are all critical skills and you probably will figure them out eventually, but that's not going to help you get that first job.

If you're not politically aware and don't know how to go ahead and communicate correctly. And then by the time you complete a four year degree,

for example, what [00:12:00] happens? You've gone through 18. 36. You've gone through two and a half G Mark cycles of things, half the things being obsolete, 50%, 25%. You're down about 17 percent of what you started learning beginning of freshman year being fully current.

think about it. 18 months ago, hardly anybody was talking about GPTs 18 months from now that Windows 10 box you're working on. It's totally obsolete. So what do we need to do? As CISOs and other industry leaders, we can take proactive steps. Number one, we have to have robust onboarding practices that have to go beyond just basic orientation.

Help our new hires learn about company specific tools and technologies, create some real world scenarios relevant to the organization, and make sure that our policies or procedures and our compliance requirements are introduced to our people early on, so they know exactly what environment they're at.

Essentially what we're finding is that we are going to be accepting [00:13:00] graduates who are not full up rounds. They need to be continually modified to get them into a functional role. Or of course you get somebody that's more senior. But the idea is that if this is a person that we want to invest in, we're going to have to spend some time between when they walk in the door and they're ready to go.

We want to have comprehensive guides for each tool in the processes and our security stack. Keep them updated, keep them accessible, and ideally have somebody who's more experienced do a little video tutorial or some interactive module to help your new people with the more complex concepts. How about this?

And this is something we used to do in the Navy. We had a buddy system. And we called it running mate. But what would happen is when a sailor would be assigned to a ship, we would identify somebody who's a little bit more senior to them, but was enough that they could still be considered a peer in a similar career path.

And that person would reach out and said, Hey, welcome to the USS Tradecraft. And we're looking forward to having you on board. And by the way, I'm going to be helping you out. And [00:14:00] I'm going to be walking you through here. And at this point in time, you're going to get that day to day guidance to support and the orientation to help people do better.

We want to have continuous learning. Make people have access to our learning and educational programs. Don't assume that when somebody shows up with a degree that they've got it all. If you as a corporation are not investing in educational programs for your people, or you say, Oh yeah, we'll let people go to one conference a year or do one CERT a year.

That's not enough. You need to do continuous learning. Much like we have this continuous monitoring. we want to rotate people. in different positions because we might find out that the job we hired him for may not be where they're best at. We might've thought that they fit over here, but they're brilliant over there.

And as a result, you have a little bit of flexibility with that. Think about having what we used to have, brown bag lunching, luncheons, or things like that, where people get together and you could learn from your peers. Instead of [00:15:00] going out for lunch, you sit around and one of the members of your team is going to go ahead and teach some concepts to everybody else.

We used to do that. And that was very helpful because. Even if you're really nice, you can go ahead and buy pizza for everybody. But the point is, let people train and work together, work with your local universities. they can always use a guest lecture and, as an adjunct faculty, it's a bit of a commitment, but if you choose to do that, you can then bring a touch of realism to the curriculum for organizations, because quite honestly, if all you've done is work in the EDU world, you might not have had to go ahead and put out a lot of the cybersecurity fires that happen in the real world.

And then have some real. tiered skill development program that's going to give us milestones. So for the first six, nine, and 12 months of employment, people know exactly where they should be. And therefore what we're going to try to do is we're going to try to reduce from about six months. to around six weeks.

The time frame it takes for a new hire to be a fully capable person. [00:16:00] Why? Because we're not going to assume they're going to figure things out on their own. We're going to go ahead and create a program. Does that take work? Yes, it does. But as a leader, that's something that you are expected to do. Now, another illusion we have is that The theory may trump practical skills.

Now there's some balance back and forth that in the academic institutions, they said you're going to lead toward theoretical concepts. Part of it is that, yes, I would say that a strong foundation in theory will prepare you for a long term career success. However, as I said, it's also a symptom of not being able to change your curriculum every semester very easily.

And as a result, you have to have something that's going to stay. Much if you're an organization that has to update policies. When I used to teach policy and I would say, how long does it take for policy to get approved in your organization? And three months, four months, six months. And one person who worked over in, nuclear industry said, Two years.

So two years. Yeah. Any change in [00:17:00] policy is going to require at least a two year cycle before it comes through. if you're going to be having to write cybersecurity policies that will take two years to adjust, do you want to be very specific or do you want to be very general? it's the same thing here in academia.

If you can't go ahead and change your curriculum quickly because of whatever factor, you're going to need to think about how do we do this in a way that it's going to stay valuable and relevant. And as a result, you lean toward theory and you have fewer practical skills and then graduates aren't well prepared for things such as that.

I may have mentioned one time I had talked to a lady who had just getting her cybersecurity master's degree and she had a a 4. 0 very impressive on paper anyway. And I met with her and I said, hey, let's talk a little bit about practicality. And I went through and I came up with eight questions, things that I didn't think were terribly difficult, but they were more practically oriented.

She didn't know any of it. Didn't understand networking, didn't understand packets, didn't understand how protocols work, [00:18:00] didn't understand how certain apps, and I said, I hate to break it to you, but these this organization, it took your money, but it didn't give you what you thought you had.

You got a nice diploma, you got an A. But you're going for a technical interview and you're going to bomb because you don't know any of the things that you need to know practically. you've got to be careful out there because not all these educational programs are going to give you what you need. And here's some of the misplaced focus you might have on cybersecurity education.

Okay, You have to know all these port numbers. DNS is port 53 and we have to have port 80 and okay. That was great when I run Hacker Jeopardy and I did port math, because as a category you'd have to do the math, but you don't need to know those things. If you're running Wireshark, you don't have to go ahead and know that the offset for the protocol, embedded protocol, is at byte 9 and things such as that, because that's all going to be given there for you.

But if you understand the concept of why do we have. ports. What's the difference between TCP and UDP? what's [00:19:00] security involved in things such as that? And how to analyze port related vulnerabilities? That's a little bit more beneficial. If we look at the OSI model, Physical Data Network Session Transport Presentation Application, it's not it, is it?

But it sounded good. Physical Data Network Transport Session Presentation Application. Okay, that sounds a little bit better. How can you say it backwards? Physical Data Network Transport Session Presentation Application. That was a joke. I used to do it. I was teaching it. You just turn around and say it backwards.

I think that understanding the concept of the OSI model is really important because it helps you know what takes place here and there. Let's get a little bit more specific. What's going on at Layer 2? Why is it, for example, that you're not going to see a MAC address on the other end of the communication, if I'm talking to Google, for example?

Because that doesn't go on Layer 2, but your IP address will. And do you understand why you get IP addresses that are ephemeral and they're rarely locked down? Although they are, of course, if you have something like a publicly facing server. [00:20:00] But even then, unless you're buying your IP addresses directly from an ISP, if you're going to a hosting company, that may move around a little bit.

So all these things change, and we want to make sure how people understand how different attacks could work at different layers. Password complexity standards. Uppercase, lowercase, numbers, special characters. No. Read the NIST 800 63 BRAVO. And you'll find out that they got rid of all that stuff. Why?

Because first of all, you're common. Denominator today should have absolutely nothing below MFA. In fact, Microsoft is making it absolutely mandatory. Can't get out of it unless you ask for push to the right, but they're only going to allow that for so long. They're going to require MFA for all Azure access, which is a good thing.

It's way overdue. Now, if you're not doing multi factor authentication and you're still focusing on uppercase, lowercase numbers, special characters, and things like that. You are out of sync. And so as a result, if we have good MFA, who cares about password complexity? It [00:21:00] doesn't have to change every six weeks or six months or whatever, because people are just going to go ahead

and write it down, or they're going to put a one at the end of it or something like that.

And it's not getting any better. And then also another thing from a concept is we're still thinking to a large extent on the emphasis on the perimeter security. with cloud computing, remote work, there is no clearly defined network perimeter. It's gone. zero trust architecture, cloud security models, securing distributed systems, that would be better than the perimeter security models and things like that.

So what should we prioritize in terms of education? Real world attacks. Let's understand those. Let's look at some recent major breaches, look at the TTPs, the tactics, techniques, and procedures that were used by the threat actors, and show students how to use threat intel feeds and stay up to date on emerging threats.

How about hands on experience with security tools? Go ahead and work with a Security Information and Event Management, SIEM, guess it depends on what part of the Mississippi you're from, how you pronounce that. [00:22:00] Teach students how to use the vulnerability scanners, pen testing tools, and how about capture the flag exercise, the CTS, and put that into the curriculum and make it hands on.

Learn how to build a secure system. Focus on secure coding principles and how do you put security into a software development life cycle and teach those principles of security architecture and DevSecOps for your students so they understand that you want to shift left, as we say, in terms of your security, but it all gets built in instead of, oh, we have to go ahead and paint it on afterwards.

How about mastering the fundamental safeguards by teaching risk assessment and how to prioritize security measures based on the organization's specific needs? Now, if you've got hands on experience with firewalls, IDSs, access control, et cetera, and maintain a robust program of patching and config management and user awareness training, you can go a lot farther than you will in terms of being effective than having just a basic theory [00:23:00] understanding.

And I mentioned this before, but the idea of soft skills, being able to communicate effectively to others, explain technical concepts to non technical stakeholders. That's a real value. It's Richard Feynman who said it. You want to really show you understand something, explain it like you're talking to a six year old.

And sometimes, no, no insults to managementers, but that's sometimes what you need to do is break it down in a simplistic area so that you have real world examples that you can communicate with instead of just reinforcing more and more technical stuff. Effective writing seems to be a skill that's almost lost.

when I've been around a while, so when I did my term papers back at Northwestern, we did it on a typewriter, we didn't have a word processor, we didn't have PCs, we didn't have Grammarly, we certainly didn't have generative AI and things like that. And so you had to think it out carefully because once you start typing, that's it.

If you got to go back and erase it and try, it was just a pain in the butt. what happens was, is that a lot of us back then would learn things. There's a book called [00:24:00] Strunk and White, The Essentials. I have, Style, and if you have never heard of Strunk and White, go look it up. Build that into your writing.

one of the things I would love to do when I'm hiring somebody is to say, Hey, I'd like you to write something for me. By the way, take out a piece of paper and here's your task. Write about this. What do you mean? It says you can't use the computer, you can't use the internet, you can't use Gen AI, you can't use Grammarly.

I want you to just write it. One page and on the subject. How well could you do on that? Would your handwriting be legible, but also could you be coherent in how you do things? And then being able to go ahead and put together more complex concepts and then communicate it effectively and how to go ahead and write that.

Those soft skills go a long way. Cause if you're presenting to older managers and they see that you're stumbling or using a gen AI tool, which has all kinds of bizarre, multi syllabic adjectives tacked on to every single [00:25:00] sentence, it's pretty obvious. A gen AI has been used to write something like that.

And I don't know, maybe they'll get better at it, but I just see something and I go yeah, no. And then lastly, what you want to do is make sure that people understand the concept of continuous learning. Much like we have continuous monitoring, continuous learning. Always dedicate yourself to getting more.

Had an Uber driver a few years back. I explained what I was doing for a living. He said, oh, I want to be like that. I hear cybersecurity pays a lot of money. How

do I get into it? My response was, it's like getting into the National Football League. You have a lot of talent and you work your tail off every day.

He looked at me, he's I don't want to do that. I said, nothing personal, but it's that's why he's driving an Uber. But the, the idea was, you have to invest in yourself. You can't be spending your nights partying and having fun all the time. You've got to continuously learn and you can be looking online resources, professional networks, security blogs, come to conferences, go to B sides and things like that.

And if we shift from. From theory to more practical industry aligned areas, we can [00:26:00] help the next generation better prepare for a cybersecurity career and even help them get hired in the first place. Now, once you get to the workplace, what happens? That could help your career track going forward. In a lot of organizations, there's an intense focus on performance.

It's an up or out. Microsoft under Steve Ballmer had a situation where you had to blow, bottom blow, using old Navy term, as we used to call them, but when you get all the sediment out of the bottom of the boiler, it was a bottom blow, but you bottom blow the bottom 10 percent of your performers based upon whatever scale you had.

But what if I had 10 Nobel prize winners? Sorry, the rule says you have to fire one of them every year. 'cause you can only keep the top 90%. Or also you look at Jack Welsh, known as a GE, where he had different groups where if you were in the top and I think it was 10%, then you were treated really well and made all kinds of extra bonuses.

If you're a bottom 10 or whatever that number was, then your chances are getting thrown out. it turns out that the motivation was really only at the [00:27:00] margin, because if you're at the 88 or 89, you wanna get to 90 91 and locking that bonus. And if you're at 91 or 92, you don't wanna get taken over. But if you're at 99, you're good.

Same thing if you're right down that lower edge, but if you're in that big blob in the middle and you know you're nowhere near getting a monster promotion or raise and you're nowhere near getting fired out of their bottom, it's not going to motivate you one way or the other, but new hires are going to come in there and they need some time to adjust.

And so what had happened, I know in the Navy, what we did is that for junior officers, you come as an O 1 or an O 2, we weren't even, we used to, but we

don't even rank you against your peers anymore. Used to be like, you're the number one ensign, great. What does that mean? You're 23 years old and you're better than the other 23 years old. At What?

But if we can go ahead and said, yes, you're gaining your competence, your skills, and things like that. We just want to move somebody along. Cause we're not going to fail to promote somebody from 01 to 02 or 02 to 03, except in the most egregious of circumstances. You're not going to blow your people out at the end of one [00:28:00] year saying, we hired 10 interns or we hired 10 new employees and we're only gonna keep nine of them.

Get them to the point where they should be performing and make stuff happen. Now, yeah, there's a little bit of concern about stress and burnout and things like that, because I agree. I'm used to a lot of stress and a lot of workload and somehow you get used to it, but that's. a coping mechanism that you build over time.

And not everybody comes right out of high school or college with those robust coping mechanisms. And unless they've been through some sort of opportunity, the military run them through things like a boot camp, where we put them in an artificial stress environment so that they can go ahead and produce actions.

In a shorter period of time that have to be correct and they learn and they get feedback very quickly, but we don't do that normally in the real world not suggesting that we necessarily have to go ahead and do a cyber boot camp where we go ahead and stress everybody push ups and things like just that but we ought to think of some way to help people develop at that have a Onboarding [00:29:00] process that'll help some set some realistic expectations Mentorship programs again huge mentoring to be able to go ahead and have somebody a little bit more senior Helping somebody out and creating a sort of a no fear environment.

That is to say you should be able to go to your mentor and ask questions that you think, it might be embarrassing, but I really need to know this. And as a mentor, you should accept responsibility for the success of your protege to ensure that he or she is going ahead and progressing effectively.

Cause that should be part of how the more, Senior people are evaluated at the end of the year is how well did you do your mentoring because that's part of what I need you to do if you're going to be a senior leader in my organization. And you want a culture that values learning and growth and help the fact that people take a little bit of time to develop those skills.

Some other challenges out there are limited training opportunities because let's face it, if we're cutting costs, Professional developed budgets are one of the first to get reduced. You [00:30:00] don't get to go to the external training courses. You don't get to go to the conferences. You don't get to go ahead and spit, Hey, I'm going to spend 8, 800 listening to somebody talk for five days.

Plus airfare, plus hotel, plus meals, plus, oh, by the way, you're still paying them their salary and they're away from work. That's a huge investment. Now we're talking 15, 000, 18, 000 for a one week training CERT course. And if you look at it all in, it's a big deal. And so what happens then is that organizations are going to say, we're going to just train ourselves or we're going to do something local or whatever, but it's going to start to stagnate the skills of your staff and the employee satisfaction is going to go down.

And for example, If you hire a new pen tester and you say, Hey, here's 90 grand and you can do, let's say a SANS course, I'm going to say that's 8, 500, but when you go plus, plus, it's really closer to 15, 18 grand. And after a couple of years with salary increases bonuses, you probably put in almost 200, 000 into that person all total.

And yet, [00:31:00] You may still lack some critical skills for full productivity. So we want to have internal training programs that can compliment or even replace these expensive external courses. Nothing wrong with a SANS course, excellent material. I taught for a decade there, tremendous amount of emphasis on quality in terms of their content and their construction delivery, but.

It's not the only game in town. And if you're under financial pressure, it's not a viable option for your organization. you can create online learning platforms, culture of knowledge sharing, take a look at Udemy and some other courses that are out there. Look at CISO Tradecraft. We've done over 200 episodes and we don't charge people to listen to them.

You could go ahead and binge watch these episodes or binge listen to them, depending upon how far back you go and you'll learn an awful lot. Now, is it going to be a rigorous educational program like you'd find in academia? No, we didn't build it that way. Although we are building out courseware [00:32:00] and stay tuned for that because you might find that to be very useful in the next couple months.

Sneak peek here. I just mentioned that to you buried here in the episode. But the other thing to think about is that there's a lot of practical skills and knowledge here that comes from being around for a long time. I try to share with you

insights that you're not going to get out of a textbook and you're not going to necessarily get in a edu environment.

From a professor who may be brilliant and she's got a lot of book knowledge, but might not have had to go ahead and deal with a lot of stuff in the real world. Okay. How about retention? Once we hire somebody, we train them up to speed. We've got them skilled and they're up and running. Now what happens?

Now they become more attractive to other employers cybersecurity, people can get poached all the time. You get a lucrative offer. So what makes people want to stay? Have you thought about that? How do you poach proof your people? Some organizations say, we'll make you sign a contract that if you go ahead and you go to this really expensive [00:33:00] certification course, there's a two year payback and anybody who hires you has to pay us back and maybe some depreciating schedule for the cost of that cert course.

Okay, but that just means the employer, the new one, just gonna say, all right, we'll just throw a little more money at it. How do you get your people to stay? Have you thought about that? It's more than competitive compensation packages. It's also includes career path progression, a role to work on different projects that are going to stimulate your imagination and feel excited about it.

A positive work culture that values somebody's personal contributions and you can help get a work life balance and things such as that. And so there's a lot of things that we can be able to do here. So how do we support this next generation? as I said, in addition to mentoring programs, you have an opportunity, even an obligation to create some more [00:34:00] impactive.

youth opportunities, growth opportunities for new hires. How do we involve them in new leadership activities? How about as a new hire, you come in there and you get to go ahead and take many notes. You'll get to be the scribe, if you will, for executive meeting or an offsite. And that means that you're going to be present at all the meetings.

You might have to go ahead and get coffee or things such as that. I'm not trying to say we're going to make it demeaning, but what you want to do is that what you want to come up with is figure out how can I get this person exposure, not just exposure to the ideas and the concepts that are going on, but personal exposure.

So people see who you are and being able to be seen by all these cybersecurity senior executives. On a ongoing basis for a two or three day event, they're going

to know who you are, particularly if you did a good job. You get exposure to strategic thinking, executive level communications. You get networking [00:35:00] opportunities.

You get a better concept of the concept of what's going on at the business level. And now what happens is you can get your junior people involved in drafting up executive presentations. And you know what? The first one's going to be horrible. And we know that. Write it. But I've never written it before. I know.

Write it. And then when you're done, don't tear them apart. Sit down with them and say, Okay, here's how we can make this better. Here's how we can do this. One of the things I found out in the Navy is that command was very rare to obtain. In the Navy Reserve, it was easier to get your child into Harvard than it was to get command as a commander.

It was a 6 percent selection rate for command. And what happened is if you got one of those commands, then what's the prime directive? You don't want to screw it up. And so what was happened is instead of doing your leadership role, which is mentoring and developing your people, it's Hey, give me that report.

I'm going to make sure that everything is done correctly. Oh, let me fill out this report. I got to [00:36:00] do it. Hey, let me take care of this. And so what happens then is that particular executive is so worried about his or her, Future that fails in the primary role of developing your people. And so give your people the opportunity to do that.

And I said, the secret to success in command is to know when it's okay to fail. Say that again. The secret to success is to know when it's okay to fail. And that's a leadership lesson, because when you know that if a report isn't perfect and the ship's not going to sink, don't worry about it. Let your lieutenant do it, and then we'll come back and it's all marked up, and then we, hey, try again.

You get a little bit less markup, and after third or fourth try, person's getting it right, and feeling hey, wow, I've been entrusted to this, and so empower your people. Now, don't do things that are mission critical that could go down because of a lack of expertise, but let your [00:37:00] people fail, and let them fail at things that are okay to fail at, but learn from that so they get better at what they're doing, and then gradually increase the complexity and the responsibility, the tasks you give them.

as the employee grows so that they have both the expertise, the knowledge base. And the self confidence to be successful. And that is also going to inoculate

them from other job opportunities. Because if somebody wants to go someplace and say, Hey, we'll pay you more money. do I get to do this? no.

Do that? No, but you'll do this. Make people want to stick around and you do that. By imbuing them with a number of responsibilities and opportunities to learn and to grow in those things. We can get involved with the local community. You can have participations at your ISC2 or ISSA meetings or things such as that.

And support your employees who want to present at these events. Maybe give them a 100 bonus if they get a speaking gig someplace. [00:38:00] Local. I'm not saying you need to pay him for travel, but it's local stuff. hey, I got a job. I'm speaking at B Sides or I'm speaking at ISC2, or I'm going to speak at an InfraGard.

Put in for that. We'll give you a hundred dollars. A little plus up on your check. Not a lot, but it's a nice way to say thank you. if you want to go to major security conferences, that's great. Submit talk proposals and reward those as well and create the interim opportunities. If you start to build your pipeline of talent this way by getting people out, you can showcase not only their knowledge, But your company or your organization's reputation for cybersecurity expertise, that then may attract others to want to, Hey, how do I be part of that group?

They're always speaking, they're talking about really cool stuff, and I want to be part of that. And so make sure you have some time and budget for that, that you don't have your people so scrunched in time that they're not able to do something expansive like that. And then also [00:39:00] use these opportunities, because sometimes people run across some really brilliant ideas, and you might be able to run with them.

So we have current technology, and there's new stuff that comes out all the time. And the hard part is that in a smaller organization, you tend to renew your products or services, and therefore they don't end up being changed. And you get stagnated in your skill sets. I've been doing the same thing for one year, two year, three years, as compared to bigger organizations where you can move around.

If you have pilot programs, if you have opportunities to regularly review different technologies, You can keep your people interested. And so if we go ahead and we look at how we've gone from compliance, for example, where

originally we just do manual evidence collection, and then we go ahead and we get a SOC 2, Type 2, or something like that.

And from there, we've moved on to unified control frameworks. Now we can map multiple standards. And now we've got automated evidence collection for all these existing tools. What's next? AI [00:40:00] driven compliance and monitoring. these tools, Generational changes make a difference and it gives us something more to learn.

We can engage with vendors. When vendors come in to pitch through their products, let your junior people listen in on them. not all of them, but sometimes vendors have a lot of very useful online seminars and things like that. And those become useful. And then if you're going to have somebody attend one of those on company time, there's a payback.

You've got to write up a summary. Tell me what you've learned. Share it with your team members. And oh, by the way, you can't just go ahead and have your otter AI listen to it and then spit out a bunch of notes. That's not what we're talking about. I want your brain to be engaged on that. You can see I'm still fighting a little bit about this AI thing.

And then with this regular technology review process with your team and exploring, experimenting new tools, you're going to have a culture that values innovation and continuous improvement. So let's conclude all this stuff. We're talking about what are our potential [00:41:00] obligation to our cybersecurity career pattern for our junior people.

Are we in a crisis? And if so, as a leader, what is our responsibilities? First of all, we need to address the myths. We have to take away and debunk these illusions around talent shortages and job readiness. There are jobs out there, but there's not as many as you think they are. And quite honestly, they're more of a mid level rather than entry level.

the education gap. Work with either educational institutions or certification organizations to align your curricula to new requirements that are real world. Or podcasts, things like this, where our stuff is updated. And it's real time all the time. Create meaningful experiences for your people. Get community engagement and foster a concept of continuous learning.

Edmund Burke had said the only thing necessary for the triumph of evil is for good men, considering the viewer who wrote it, to do nothing. In the context of

cybersecurity, our [00:42:00] inaction in developing the next generation could lead to vulnerabilities that malicious actors are all too ready to exploit.

By, actively being involved in nurturing new talent. We're doing more than just filling job positions. We're enhancing lives. We're increasing our collective defense against cyber threats. We can drive innovation by unlocking some brilliant minds and focus on problems that they might not have looked at otherwise and create long term sustainability of growth of the cybersecurity industry.

So reflect on these insights. Think about what we put together in this episode and whether you're a CISO or a team leader, individual contributor, how could you implement these ideas in your organization and nurture the next generation of cybersecurity professionals. If you're a leader, how do you create more meaningful development opportunities for your junior staff?

If you're earlier in your career, how can you seek out growth experiences? and contribute to your local cybersecurity community. It's like the advice that I got when I first started [00:43:00] at Booz Allen. Speak every chance you get. That was Lorena Lemons. And I did. My first speaking gig was with Admiral Grace Hopper, coincidentally, which is pretty cool.

But I have spoken over 1, 000 times. And when you start doing it, you start to learn an awful lot, and you learn how to communicate. And you can create great things and a name for yourself in the industry. So share your thoughts, experiences, and address this, and then work together with your teams and your senior management to make sure that you can create a successful environment so that you can bring on board and then grow our next generation of cybersecurity professionals and do it in a way.

That creates job satisfaction, personal satisfaction. You will be corporate satisfaction. Cause these people aren't going to want to leave because this is a really cool place. They invest in me. They trust me. They give me an opportunity to try stuff and that's going to give you a competitive advantage.

And by doing this, I think we're going to have a really bright future for [00:44:00] cybersecurity. And for those of us who've been around a long time, it makes us wish we were 20 years younger. So we'd have a lot more runway, but we've blazed a lot of trails for everybody. And we hope that the career paths that are available to folks today are as exciting for them as cybersecurity was for us back in the early days. So thank you again for listening to CISO Tradecraft. If

you enjoy our show, please give us a thumbs up or a five if you're listening to us on a podcast channel so that what? We can get other people to get attracted to it.

Check us out on YouTube. We're a little bit lagging on our YouTube numbers, but you don't get to see a whole lot of you hear the same thing. I'm not using slides or anything like that, but I would appreciate if you take a moment, follow us on YouTube. So we could go ahead, and it helps us get rid of those stupid ads that they throw at you.

Because once you get enough, followers, you get control over that. And we're not trying to push ads in your face. I'm actually trying to get rid of them. And then share with your peers and share with other people to help them find places that they can grow their cyber security career paths. So stay vigilant, stay curious.

Let's work [00:45:00] together and help solve this problem together. And until next time, it's your host G Mark Hardy. Stay safe out there.