Podcast 144 Tyler Leet CSI

May 2023

By Tyler Leet

Lisa Hochgraf 00:04
You're listening to the CUES Podcast episode 144.

Lisa Hochgraf 00:08
Welcome to the CUES Podcast where leaders and experts discuss the top topics in credit unions today.

Lisa Hochgraf 00:14
I'm Lisa Hochgraf, senior editor at CUES and your host for this episode.

Lisa Hochgraf 00:19
Readers of CUES' Credit Union Management magazine told us in our most recent survey that cybersecurity is among the top challenges credit union leaders face today. This conversation with Tyler Leet will give you lots of concrete things to mitigate the risks of cybersecurity. You'll sleep better after you listen, because you'll know you've applied best practices to mitigating the right risks.

Lisa Hochgraf 00:43
Tyler is the director of risk and compliance services for the regulatory compliance group for CSI, the sponsor of the show. A self-described "techie," Tyler not only loves this stuff, he also has more than 20 years of experience in the information security risk and compliance industry. His advisory work has included leading the development, implementation and maintenance of risk- and compliance-related services for a wide variety of financial institutions.

Lisa Hochgraf 01:13
In today's show, Tyler talks about key differences between vulnerability assessments and penetration testing, as well as between compliance and security. Plus, he explains why you need to consider all these things to succeed in building a well-balanced cybersecurity program that will help your credit union mitigate the risk from financial and reputational damage associated with cybercrime.

Lisa Hochgraf 01:37
The show also gets into why credit unions need to stay current on not only what hackers are doing, but also regulations and the innovative tools available to help them mitigate cyber risk; how to think about your credit union's network broadly, so you can better defend member and organizational data; how to put vulnerability assessment results into context; key elements to include in your credit union's cybersecurity plan; and why investing in cybersecurity pays off.

Lisa Hochgraf 02:07

I bet you're ready to hear from Tyler, and sleep better tonight. So let's get started.

Lisa Hochgraf 02:15
Welcome to the show, Tyler.

Tyler Leet 02:17
Thank you very much; appreciate you having me, Lisa.

Lisa Hochgraf 02:20
I'm really looking forward to talking with you a bit about offensive security today. But before we jump into that, I'd like to help our listeners get to know you a little bit. And to that end, would you have a quote or a mantra that you use to guide your professional life that you could share?

Tyler Leet 02:37
Sure, I think one that comes to mind both professionally and personally, I say it to my sons oftentimes, is do what you say you're going to do. Be a person of your word. Follow through, that kind of thing.

Tyler Leet 02:50
I guess a close second, if not potentially a first would be, if you're going to do something, do it right. So I think those are two that are very close to my heart.

Lisa Hochgraf 03:00
Uh huh. Yeah, I can see both of those applying to security too.

Tyler Leet 03:05
Yeah, they're pretty important. You don't want to really take any shortcuts on doing things correctly in security. I mean, you can but in, in reality, it's probably going to come back to bite you and, and cause more problems than the time-savings were worth. So

Lisa Hochgraf 03:21
I feel like both of those things were up in the karate dojo where my son studied for a long time. They're really good life lessons.

Tyler Leet 03:28
Yeah, I'm in they pretty much apply to everything I believe, personal, professional. Just I think it's a good characteristic to build.

Lisa Hochgraf 03:37
Wonderful. So let's, let's take a jump now into today's topic of security and being on offense. What is the range of possibilities of what it could look like when a credit union acts on the idea of the old adage, "a good offense is the best defense."

Tyler Leet 03:54

The offensive security field is not really new, per se, but it is certainly growing in how much it's being adopted across the industry. I mean, hackers have done this type of thing, but it's leveraging and learning from their abilities, and how you defend against that. So I would say a good offense is part of a good defense would be the way I would phrase that it's not the only thing but seeing how your defenses hold up, learning how you can reflect, react, how things are going to work, are they going to work the way you think they should? Just like the old testing with an audit, you think something's supposed to work that way but you don't ever test it, how do you know that's the case? So it lets you kind of find and poke at those potential vulnerabilities before a real bad guy does and that gives you the opportunity to close those up and make those improvements. So, certainly recommend taking an offensive approach, and examiners are starting to adopt that as well, which is good. They're starting to say see those expectations of conducting penetration tests, conduct regular vulnerability scans, that kind of thing. Because you don't know what you don't know. And if you don't look for it, you're not going to find it more than likely.

Lisa Hochgraf 05:09
I love the idea that the good offense is, is a part of a good defense and to keep up with the trends, right? What are the bad guys doing so that you know, and then incorporating that into your testing and planning? Sounds really good.

Lisa Hochgraf 05:24
So Tyler, the video on your website about offensive security talks about managing and measuring network risk, and that in my reporter brain brings up two questions.

Lisa Hochgraf 05:37
First, what do you include in your definition of network? And second, how do you go about measuring network risk?

Tyler Leet 05:44
So we'll look at it from a conceptual standpoint, and then how we kind of termed it from our services. So conceptually, as an organization, your network is: Anything your data touches is part of your network is what you should consider that. Now, that it even goes into, to an extent your third parties, your vendors, that kind of thing. And that's where you talk about, you've heard the data flow diagrams and where your data is going and coming.

Tyler Leet 06:10
Now you only have so much visibility up to their perimeters, but they are an extension of your network. So a true holistic approach you want to consider your network is anywhere your data travels, I mean, that's the safest way to look at it. Now, if you look at it from that paradigm alone, that scope is going to be quite large. So it's gonna be hard to test all of that, especially vendor networks.

Tyler Leet 06:34
Now, what we do from the offensive security perspective is we break it down into two components. We do an internal network, which is that soft, gooshy internal perimeter, that inside of your firewalls, that kind of stuff, where your employees reside, all the computers, the laptops that are used, the servers,

and then we do a perimeter perspective. So what the world sees, what are the boundaries, those IP addresses, those services that the world can access, and then we have testing for both of those. So one is that external penetration testing, and then we have the internal penetration testing. So that's, that's kind of the the simplistic way we break that down. And to make it a little bit more bite size, and digestible with conducting the testing.

Tyler Leet 07:19
As far as measuring risk, a lot of that is actually done based off vulnerabilities by the those experts that are out there with the CVSS scores, that kind of thing, vulnerabilities by default anymore, given ratings of their criticality, which take into consideration various factors, as far as what can be accomplished is that theoretical, that kind of stuff. That said, context-- looking at all vulnerabilities in context is very important. Just because a vulnerability might say it's critical from a provider, you might have certain controls on your network that make exploiting or executing that vulnerability nearly impossible for other means. So in context, it brings that risk down.

Tyler Leet 08:05
So what we kind of do is look at what's there. What's the default score of a vulnerability like that, but based off everything else, we see that you have in place, how much more difficult is it for an attacker to execute something like that, which is a remediation, a mitigating control, to bring that risk down to more acceptable levels.

Lisa Hochgraf 08:26
Two follow up questions on that Tyler. One question is, when you say that a network includes every place that your credit union's data reaches, does that include members' cellphones?

Tyler Leet 08:39
No, you there's a realistic, that was more of an abstract thought component, when you're thinking like it as an organization, you have to think of where could our data be compromised. Yes, it could be compromised from a member's cell phone, but you don't have control of that. So in terms of what the organization needs to look at, you want to look at anything that extends potentially out to those outside entities because you can't control what's in the outside entities but knowing where it's going and then what you can control up to those points is the important part of what is considered your network.

Tyler Leet 09:17
Now, granted, that is, like I said, a very abstract way to think about it from a larger perspective. But realistically, if you don't know every way your data's going and ensuring that what you have control of along that path, you should do everything you can to protect that. Now beyond your scope, beyond your reach, you can't do anything there. But you talk about the cell phone, for example. Yes, you can't can directly control the user cell phone. But if you're interacting, you can ensure your systems, the communications going there, are they encrypted? Are the applications you're using to get them there encrypted with proper encryption protocols. Are there good authentication mechanisms where if their phone is compromised, you've got a two factor or something else that can keep an attacker off of your systems to keep that transition from happening from their cell phone to your system and data? So it's

looking at it from a larger picture about how those third parties could potentially affect your network and your data.

Lisa Hochgraf 10:16
That's great. Thanks for the clarification. And I think you mentioned something like CVSS assessment. Is that, did I catch the acronym right there? And can you tell us a little bit more about that if I did? Or can you correct it if I didn't?

Tyler Leet 10:29
It's a CVSS is a, it's called the common vulnerability scoring system is what that stands for. It's a an industry standard. There's actually been several versions of it. There's a, they still offer version two and version three, oftentimes on vulnerabilities when they're scored. That's like an industry accepted standard, that pretty much any vulnerability that's identified, is given one of those scores, and there's a number of factors that it looks at as far as like the criticality of what can be affected, how easy it is to exploit, how widespread it might be. On the internet, there's a number of things that they go into that scoring. It is, if you ever look at a vulnerability scanning report, wherever whatever vulnerability scanner you might use, you will see the acronym CVSS score and there's a version two, version three, and it lets you do on a one a one to 10 scale. What is that criticality? Like how, how threatening is that vulnerability, potentially, to your network based off of just a default set of factors.

Lisa Hochgraf 11:33
That has to be super helpful to have sort of a standard score that can put things into perspective as you're, as you're measuring and aligning priorities? So

Tyler Leet 11:43
Yeah, absolutely.

Lisa Hochgraf 11:44
Can you give me some examples, if you got a result on your scoring system, like, what you do and what recommendations you might make based on the results that you got?

Tyler Leet 11:54
Well, in terms of what the CVSS score alone, I would always say, you want to look at anything that's for sure high risk and above. And I actually recommend you looking at the moderates, like going through all identifying all moderates and above, and then actually performing an assessment on what the rating is because there's a difference between a vulnerability scan and a vulnerability assessment. A scan is just okay, let me point my software at your systems, run it, see what comes back. Okay. Well, that's done. That's a vulnerability scan. Assessment is adding that context that I mentioned, looking at it and saying, okay, yes, we've got this vulnerability. But we've got X, Y and Z controls in place, which makes it a lot harder to execute this vulnerability. So let's move it down a little bit on the priority list of things to get fixed. Because it's got more controls in place, as opposed to vulnerability No. 2 over here, that is much more exposed, we've got a lot of data there, even though it CVSS scores a little bit lower, there's a bigger risk for us there. So that context makes all the difference. That's the assessment component, looking at the exploitability of it, and the exposure that your organization has with that vulnerability.

Tyler Leet 13:12
Now, that's from a vulnerability perspective. Penetration testing, a good penetration test, might have vulnerability scans with it, but a good penetration test, the attackers are going to be as quiet as possible because you want to simulate the full attack. A good hacker is not going to get in and run a vulnerability scan because that's going to like set off in a lot of places, alarm bells, like 'I'm here, like, look at me, like somebody's trying to do something in your network.' So while we do a vulnerability assessment at the end of a penetration test, we start off trying not to be seen and noticed. So you do things very low and slow, creep along, try to gather information and grab those footholds.

Tyler Leet 13:52
Ultimately, especially for first-time clients, we usually reach our goal of the test, which the common goal, by and large for an internal test is domain admin. We take over their network pretty much every time in the initial tests because it's very eye-opening to see how many ways there are to gain access to a network, administrative access, and by and large, it comes down to weak passwords.

Lisa Hochgraf 14:21
That's all really interesting. I like the idea of taking the initial score, putting it into context, testing based on that. And then I'm also really interested in what you're saying, which is that you come at this kind of from a couple of angles, right? You do the assessments and the context and then you also do a pen test. It's like the we used to talk about layered security years ago and I I still think there's value in coming at it from different perspectives and different ways.

Tyler Leet 14:49
Yeah, absolutely. I mean, layered security, still defense in depth, layered security, still very valid, and highly recommended approaches, but in terms of offensive security, and that's, this is a common thing, glad we have an audience for this. Vulnerability scanning and penetration testing are two different things, but they're oftentimes incorrectly used interchangeably. And sometimes you're responsibly sold with the wrong label from a vendor, as a vulnerability scan is very simple. I mean, anybody can get the software, scan and get results. A penetration test is much more manual. A good penetration test, should be able to do that without using any commercial software. You should be able to do it with free tools that had been made by hackers and other people on the internet without having to purchase a single license. Now, you can combine the two and make it much more thorough.

Tyler Leet 15:52
But vulnerability scanning and penetration testing, very important to know those are very different. One is large, kind of spray and pray. That's the vulnerability, try to find as much as you can, in as quickly a quick amount of time as you can. Without context, the other is very object-oriented. We're trying to do this. We're going to take particular steps in order to try to achieve this goal and see what we can find along the way.

Lisa Hochgraf 16:15
Excellent. Thank you for that clarity. I keep using clarity. But it's so important that credit unions understand the details of this because cybersecurity is what's keeping them up at night. No question.

Lisa Hochgraf 16:25
So another concern in this space that I hear about a lot is the credit union that says "Oh, well, I'm compliant. So I'm all set." But I think maybe best practices and regulations, while sometimes parallel, compliance typically doesn't equal secure. So what are your maybe one to three top recommendations for credit unions, when it comes to being on the offense against digital thieves? And I'm assuming No. 1 is not be compliant?

Tyler Leet 16:52
Yeah. I mean, I'm very appreciative of the fact that you brought this up as a question because compliance does not equal security. Compliance is a minimum baseline for security. It's not necessarily security. It's like, okay, this is the minimum standard we need you to meet. And in comparison, we'll give credit where credit is due, if you look at verticals across various lines of business, financial institutions, because they're regulated, and they have that level of compliance, they are compromised on a much lower frequency with a lesser degree of compromised data than the other verticals out there that do not have that. So it pays off. It is paying off. It might not feel like it, but it is.

Tyler Leet 17:35
But that being said, yes, just meeting those minimum compliance threshold is not does not mean your organization is secure. There are other things you should do to be secure. And I think, in large part, more organizations are now starting to think about, yes, security does not make money. But it's much like insurance. It saves you money, potentially, in the long run and can potentially save your business under certain circumstances. Because small businesses, it's been found that you could ransomware or breach, I don't remember what the statistic is, offhand. But it was a vast majority of small businesses do not recover if something like that were to happen to their organization.

Lisa Hochgraf 18:16
There's a huge reputational cost too.

Tyler Leet 18:19
Oh, absolutely. Yeah. Reputation, as everybody knows, takes a long time to build, like trust. I mean, it's a form of trust, takes a long time to build, but it can be dismantled very, very quickly. And especially with the internet and the way word spreads, news spreads today, and can people can easily share their opinions about things. However informed they may or may not be. That's an even greater degree. It's ah instantaneous anymore, as opposed to back when and we just had newspapers and word of mouth and that kind of stuff, for any of our listeners that remember those remember those days when you didn't have the internet to see things instantaneously? So it's a different world in that regard.

Lisa Hochgraf 19:04
So what would you say? What are the top one to three things that you would recommend credit unions do in this kind of murky mess of cybersecurity.

Tyler Leet 19:13

We're on the topic of the offensive security. So I mean, I'll de facto go to this, but you can't be scared of the results. You want to find that type of thing. You want somebody to come in and be able to find this because you'd rather that person be doing it than an actual hacker. Yes, you might not like it if they come in and take over your network. But ultimately, if you think about it in the longer the longer scheme, you can fix that, you can use that information to improve, and it's not a real bad guy. So don't be scared of those results. I mean, you're doing this. It's not like a pass/fail in that regard. It's an improvement exercise. It's not something that you're looking to say, "Well, we were failures." No, you're looking at it to improve. That's the purpose of the testing. And a good provider will give context to that. This is how you can improve, this is what we did and give you kind of coaching steps to improve your your network. And the defense is there so you can make it stronger.

Tyler Leet 20:09
Another recommendation, which is, I'll say a large, this is even beyond the offensive security scope. But in terms of when I, when I get asked what's kind of the biggest-bang-for-your-buck security control, educating your users is one of the most cost effective things because oftentimes attacks leverage social engineering to a certain degree, or they rely on a user running something they shouldn't, or going places they shouldn't, or using bad passwords, that kind of thing. You can educate your members as well as your employees for a relatively cheap cost, especially in comparison to all the software and hardware out there in the security space. And it is relevant to pretty much every type of attack vector to some degree that's out there. So user education, both from your member perspective and internally can pay huge dividends for a very small cost. That's those are two that I'd recommend.

Tyler Leet 21:09
And then I think a third related to the offensive security space would be, I mean, invest in regular good vulnerability and patch management. Duck regular scans. And when I say regular, at least monthly, if you have your own software, like get the software, run it monthly, have it do the patches, make sure you're up on that because most of the hackers that are out there are not, you don't have a nation-state coming after you or somebody from a hacking organization like anonymous, where they're, you've got these super-skilled hackers that are coming after your organization. Yes, that does happen. But the vast majority of the ones out there use free tools that have been developed by a real hacker, and they're taking advantage of vulnerabilities that are on your system. And if you close those vulnerabilities off, they don't have a way to get in your system. They want low-hanging fruit.

Tyler Leet 22:06
A good patch management and vulnerability management program will minimize the surface area and the attack exposure that you have. Vulnerable systems are one of the top ways that a compromise takes place along with like social engineering, that kind of thing. So closing up those known holes. That should be an easy, low-hanging fruit for you as an organization.

Lisa Hochgraf 22:35
Yeah, I think that's well said right? Keeping up with with with the times means partly knowing what the hackers are doing, but also just working with a software to keep it as solid as it can be right? Changing mind. My machine's updating all the time.

Tyler Leet 22:49
Yeah, it's it can be an inconvenience. But there are if it's well organized, you can minimize that inconvenience, like there are things that can help streamline and improve that. But yeah, software, it's not going to go away. I mean, we get more and more software. Software gets bigger and bigger and bigger. It's not getting smaller and smaller and smaller. So there

Lisa Hochgraf 23:07
Doesn't it though.

23:08
So it's something that we as people and as businesses need to adapt, to say this is not necessarily going to improve drastically. It's isn't going to go away for sure. It's just going to be more and more of an important thing because information in the digital world is interconnectivity of systems. That's not going anywhere, anytime soon.

Lisa Hochgraf 23:28
So this next question that I had planned, you may have already given us some of the elements. But I was curious, when you help credit unions write a cybersecurity plan, what are some of the key components that you encourage them to include in that? And maybe some of them repeat? Or maybe there's some new thoughts here.

Tyler Leet 23:44
Well, we talked about the training, user education. I mean, that's one of the very important things. One thing that's also super important in today's world from a cybersecurity perspective is board and senior management involvement or higher-level involvement. Security is not just an IT concern anymore. It used to be like security was like the IT manager. Well, he's, that's their job is to keep us secure. Security is a business concern. I mean, it should be a business concern. It has a potential high financial cost for an organization if there's bad security, and anymore, we have an obligation. Businesses have an obligation. Credit unions have an obligation to keep their members secure, their data secure, their money secure. And part of that is in from an information technology, not just a cash component. So, senior management that is invested in understanding you don't have to be as they don't have to be subject matter experts, but they need to be able to ask credible questions that can challenge their IT folks, their security folks, as far as, "Is this the right direction? Are we supposed to be doing this" and coming to a complete conclusion to say, "Yes, okay, I think this is a good idea. Let's move forward with that" and incorporating that in your strategy, your business strategy is very important. Otherwise, if you don't kind of build it in with that train of thought, you're setting yourself up to fail down the road because either you're going to try to retroactively working in, which makes it really hard. Or if you just continue to neglect it, well, bad things will eventually happen. So I think that's a very important thing is that high-level, senior-level involvement, and getting them invested in understanding the importance, backing initiatives and incorporating that as a key business component of the business as opposed to just a backburner thing like it used to be 10-20 years ago.

Tyler Leet 25:40

And we talked about the regular testing, as opposed to whether it's the scans, the patch management, the user training. A lot of people balk about this as well. But risk assessments, if done properly, are incredibly important. And actually, it's a key component of the cybersecurity plan. But a true risk assessment, if you do it properly, it's not just an exercise where you're wasting time filling out an Excel Excel spreadsheet, which is what oftentimes people think about. A good risk assessment, if done properly, lets you well, one, it's a mental exercise. It's not all about it's not about the document you're producing on the end in reality. It's about what you're learning along the way as you produce that document. Identifying okay, what are our assets, letting you see what your assets are knowing for a minute, oh, I didn't think about this. This is something we need to protect. What controls do we have in place for those assets? What are the things that could come after those? It's learning those steps along the way, and how they kind of work together.

Tyler Leet 26:44
And then yes, you will ultimately have your risk assessment document, which, in the end, if you've done a good job, and given good, good thought to it, will help you prioritize your resources that are much more limited, because you can say, "Okay, we've got X,Y and Z assets. Based off our classifications, these this is the order of their importance. This is the order of where we've how good at we think our controls are. So we know that while x is the most critical asset, we've got all kinds of controls in place for it. But y is very shortly behind in terms of its criticality, but we don't have very many controls and part of it. So we need to put more controls on y. But if you were to just to look at it from an outside perspective, without having done that risk assessment, you're gonna say, "Oh, x is our most important thing, we put our controls there." But the risk assessment can show you that y is what really needs to have the controls. That's where you will optimize your bang for your buck as far as minimizing your risk.

Lisa Hochgraf 27:42
Thank you so much for all these great insights. As a someone who works for a learning organization like CUES, I appreciate the perspective that doing all of this assessing and testing has to do with learning, right? If someone actually takes control of your system, that's not great. But you get to learn a lot. And as you do all of these assessments, you learn what's going on. And that can help inform your priority-setting. Love that. Love that framework.

Tyler Leet 28:09
That's just the thing in life. I mean, you can't have successes without failures. If you don't learn from your failures, if you don't learn from things, I mean, the mistakes things that happen. And then not everything's a failure, not to say everything's a failure, but you should always be learning in life. I mean, that's if you quit learning. I mean, what's the point? At that point? You're just kind of floating in space it seems like. So that, yeah, it's a learning exercise. I mean you're looking to improve. It's not about just making the document to make examiners happy. It's what are we figuring out along the way? What insights are we gaining into our organization?

Lisa Hochgraf 28:45
Love it. I really appreciate you being on the show. And I want to be respectful of your time. But before we wrap up, what is a question that I didn't ask you that you would like to answer for our listeners?

Tyler Leet 28:57
The one thing I would say to listeners is, just because your job is not it, your security doesn't mean you do not play a role in security. You are an end user, whether you're a teller or a loan officer or an executive. You have access to systems and you are a potential target. You are a potential avenue into that network and can make a mistake that could cost your organization. So while you're not expected to be a security expert, you can learn basics about good security hygiene and to avoid being one of the reasons your organization gets compromised.

Lisa Hochgraf 29:40
Thank you so much for being on the show, Tyler.

Tyler Leet 29:43
Well, thank you. I appreciate you having me. It's been a pleasure and hopefully had some decent insights to share between my ramblings

Lisa Hochgraf 29:51
For sure.

Tyler Leet 29:51
Right, thank you very much.

Lisa Hochgraf 29:55
I would like to thank you, our listeners for taking time out of your busy schedules to listen to today's episode of the CUES Podcast. And many thanks to Tyler for sharing his expertise, and to CSI for sponsoring today's episode.

Lisa Hochgraf 30:08
Learn more about CSI's compliance and risk advisory services at CSI web.com That's c-s-i-w-e-b.com.

Lisa Hochgraf 30:19
Find a full transcript of this episode at CUmanagement.com/podcast 144. You can also find more great credit union specific content at CU management.com.

Lisa Hochgraf 30:31
Thanks again for listening today.

Lisa Hochgraf 30:33
CUES is an international credit union association that champions and delivers effective talent development solutions for executives, staff and boards to drive organizational success.