#150 - Measuring Results

[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 I want to have an important discussion on measuring results in cybersecurity. Now, I've spent over 30 years in this field, and I've worked with organizations Government, military, civilian, corporate, non profit, trying to enhance your security posture.

So in this talk, let's explore why measuring results in cybersecurity is critical, the various methods and metrics and challenges faced, and perhaps a path forward. Now this podcast was largely inspired by the Measuring Results Cheat Sheet that was created by Justin Mecham and his LinkedIn page. We'll put that in the notes.

It's based on a number [00:01:00] of sources, including a Harvard Business Review study that says if you follow these recommendations, you're likely to have 10 times more growth and results than perhaps those who do not. And so, as I said, we'll provide a link for that in our show notes, but it's https://www.linkedin.com/in/justinmecham/.

I am aware that Douglas Hubbard and Richard Seiersen wrote How to Measure Anything in Cybersecurity Risk, and that is a well respected book. I may get them on the show at a later date, but I want to limit our focus to what Justin has put out on LinkedIn so we can keep a focus on this episode. But before we get into it, let's take a moment and listen to a message from our sponsor.

Risk3Sixty is a cybersecurity technology and consulting firm that works with high growth technology firms to help leaders build, manage, and certify security, privacy, and compliance programs. They publish weekly thought leadership, webinars, and downloadable resources such as their PCI compliance program workbook, a business case for SOC 2, ISO 27001, The Path of Certification, [00:02:00] and many more titles, all available for download at no charge at Risk3Sixty.Com/Resources. Let Risk3Sixty help you build your business case to achieve certification compliance. That's Risk3Sixty.Com/Resources alright, back to measurement. Let's delve into why measuring results in cybersecurity is so important. Your goal in any organization is to create value.

Just think about it. A company's decided to pay your salary, your health care, and your retirement benefits. That costs money, and since companies are generally not stupid, they believe that this cost is going to be far less than the value you provide to the company. In a way, that's why you still have a job.

So you need to demonstrate that you are providing value that exceeds the cost of retaining you at the company. And this is how you're going to be measured. Now, we know that we need to provide substantial value to the organization. Let's consider how we could do so. Now, organizations and [00:03:00] bosses in general don't care how busy you are.

They care about the impact you make. For example, if you spend a lot of hours on an initiative that isn't important, then your results won't be much to show at the end of the year come performance reviews. The first thing is figuring out what is important. The good thing is you don't have to produce that yourself.

You can talk to your boss and the executives around the company and ask simple questions. For example, I want you to imagine we're here one year in the future. What tasks, if completed, would make you happy? that you hired me for this role. And you see, that type of question can elicit clear goals and objectives of what you need to accomplish.

Now, once you flesh those items out, you need to make them SMART goals. S M A R T. Specific, Measurable, Achievable, Relevant, and Time bound. Now, specific means they need to be clear and precise. For example, to say, We're going to build a secure organization. That's kind of vague. And the same thing can be stating that We want everybody to be aware of cybersecurity.

That's not clear or precise. So let's [00:04:00] rephrase that to say that we shall become compliant with ISO 27001 or CMMC Level 1 for a defense contractor. That's a very specific standard with clear requirements and that specificity helps us know what it is we're going for. Next, we want things to be measurable.

Things should be quantifiable and trackable. For example, if we say we want people to be aware of phishing attacks. That's not measurable. So let's reframe that one as well. We'll institute monthly phishing exercises on each of those exercises we want every division or organization to have less than a 3 percent click through on phishing emails.

And in addition, we want more than 50 percent to report a phishing email to the cybersecurity team so we can block it across the enterprise. Now this is something you can track each month through your metrics report to the

executive team. Remember, when you create measurability, You can also gamify it.

The team that does the best gets a reward. It could be a small trophy, special lunch with a CEO, probably not with a CISO, or [00:05:00] some type of recognition. But when you do this, people get excited about winning, and the metrics will move you in a favorable direction. Next, we need to make goals achievable. They should be realistic and doable.

If you're at a 10 percent Phishing click rate right now, don't expect the organization to get to 1 percent overnight. See, repetition is a law of learning. Set something that is ambitious and achievable, so perhaps you get to 5 percent click through rate in the next 6 to 12 months. Well, 6 to 12 months isn't specific, so let's make it say.

It's twice as good as you are now. And then allow people time to change their focus. Remember, if the goal is too hard, people may ignore it altogether. Just think about weight loss. If the goal is to lose five pounds, you have a competition in the office. Most people say, yeah, it isn't too hard. I can do that.

But if the goal is to lose 50 pounds. Well, that's a lot. That's too much effort. And I don't think I can do that. And I got other things going on. And, and so it's not going to happen for most people. So find the balance and socialize it with others. And that way they can buy into the experience. Next, we [00:06:00] want our goals to be relevant.

They should be pertinent and meaningful. People hate busy work. It doesn't create value. Make sure the things that people are focused on create impact. Now, what does that look like? Stopping threats that could create material impact, for example. Keeping people vigilant to report phishing attacks. Keeping software patched to avoid old versions with known vulnerabilities.

Making sure the organization uses secure configurations. Ensuring the IT team produces evidence that's needed for auditors and regulators. Each of these things ties back to something of value. And finally, smart goals need to be time bound. If you don't know when you'll achieve a goal, there isn't any pressure to make it happen.

That's why escape rooms are so popular. Escape rooms have players go into an exercise, they complete a certain number of tasks or puzzles in a limited amount of time. And this means there's a countdown timer that says if you don't get all

the puzzles complete within this time period, you lose. Now if you do complete them all, you win.

Now we need the same thing in our organizations. Is there a specific date when you expect [00:07:00] all systems to get their patching numbers in line with a specific target? 30 days? 60 days? It's about the end of the year. If you have clear due dates, then you can hold people accountable. The way I'm going to rate you at the end of the year is by your ability to hit these key goals and metrics.

If you meet them, you're successful. And if you exceed them, you could be rewarded with bonuses. So let's work on this together and we can create success. So now that we understand a SMART goal, specific, measurable, achievable, realistic. Time bound. Let's take a look at how we create key performance indicators or KPIs.

These should be things that track progress. Remember, indicators can be either leading indicators or lagging indicators. Think about like a basketball game. The game of basketball, there's a scoreboard. And the scoreboard shows which team is currently ahead or if there's a tie or somebody's behind. You could look up and say, Hey, if we keep this up, we're going to lose.

And that helps create additional motivation. So consider creating a balanced scorecard with a few important metrics that tell the story that you are following to create [00:08:00] substantial value to the organization. For example, you might say we believe the most common ways that companies get hacked are people clicking on phishing emails, unpatched software that gets exploited, third parties losing our data, or bad configurations of cloud software. Alright, given these four issues, we've created indicators that we're going to baseline our organization against each month and measure progress. Each metric will tell a few things. One is it tells the status of where we are right now.

Next, you'll see that metric from each of the previous months, and that way when we see we're patching at 60 days, is that number good or bad? Think about it this way. If last year your organization only patched as fast as 180 days, and now you're at 60, you'd probably be happy with that number. But if your organization was previously patching at 30 days or less, and now your monthly metric is at 60, you're not as impressed.

You're probably gonna ask about what went wrong. So knowing the trend of a metric is really important, And finally, we have to have desired goals that say we'll be happy when our metric hits this certain number. If you're patching

[00:09:00] at 60 days and your goal is to get to 30 days by year end, does each month show you're getting closer, farther, or staying stagnant with your goal?

And that allows you to say we're on track, or we need more focus, or more attention, or more resources. to achieve this key performance indicator. Now, once you start tracking a number of indicators, it's easy to get overwhelmed. If you track 200 metrics, nothing's important. However, if you say these are the top 10 metrics that will be reviewed by the executive team, well, that'll put focus on what things are going to be prioritized.

Remember that which gets measured, gets done. And that's what gets done, gets funded. So, don't dilute your value. One model that you can use is the WOOP model. It stands for Wish, Outcome, Obstacle, and Plan. Wish is, what do I want to achieve? Outcome is, why do I want this? Obstacle is what might block me, and plan is how can I get what I need.

Now you can use this model to show why your KPIs create substantial value. And if they don't do that, they're probably the wrong focus. Now as you start going [00:10:00] down the process of analyzing your organization's ability to achieve results, you usually see a few things. One is a gap analysis.

Here's where we are today. Here's where we want to be. There are probably some things that you want to do that you aren't doing today. So, that's a gap you want to work on. Each gap might require new tools, better processes, or focus from people to improve. Remember, it doesn't do any good to say, Here's an important metric of which we're falling short every month.

No, you need to put in the analysis for the reasons. This is why we're falling short. What steps could we take to address this gap that could change the metric? And this allows managers the ability to make informed decisions. You might observe that management wants to buy people to spend five hours patching this vulnerability.

Well, if I do that, then I lose the opportunity to spend five hours making improvements somewhere else. Now, it's a decision that needs to be made. And then it comes back to what's the priority of the organization and what's non negotiable. Perhaps the non negotiable is we will follow the security policies.

Well, perhaps your policies, they're more like guidelines, right? They're not non negotiable. [00:11:00] That's where the culture of an organization comes into play. You need to understand those things and find ways to push that work within the culture. It might start with changing people's beliefs of being non

compliant ultimately has significant negative consequences. For example, public companies in the United States must meet Sarbanes Oxley or SOX compliance requirements. That is, applications that impact the balance sheet and then ultimately the reportable financials need to have evidence that they're following IT controls.

If the teams don't provide the evidence, then an auditor is going to create a finding saying application XYZ didn't follow control ABC. It's going to be reported ultimately to the SEC if it gets all the way up there. I want you to know that the CFO... And the CIO have expressed concern and that they hate to report that we don't follow basic controls on our financially significant applications.

Because that goes to the CEO and it goes to the board and it gets ugly very quickly. So, here's what we're going to do. We're going to use a scheduling tool that's going to remind everyone [00:12:00] what's due 90 days before the final due date. And that's when we want you to begin submitting your evidence. And 60 days out, if we haven't seen evidence submitted, we're going to follow up with the control owner and their manager.

And then 30 days out, we're going to bring this up to the audit committee. And that way, everybody shares the same understanding of what we're going to report to our regulators before we send those reports out. We think this is important. We'd love to tell everyone what a great job you're doing and that we have zero reportable findings.

So if you follow this schedule... This could work. So how can we work together to ensure this happens? You see, you want to create this sort of a positive cooperative, but still hold people accountable. Now, let's just say the root problem continues and you still have an issue. Well, this is where performing a root cause analysis using five whys is a good thing to consider.

Ask why five times. I mean, let's say you need every application team to ensure they remove access in a timely manner when someone leaves the company. Why? Well, because you don't want people who have left the company to get access. But every year there's two to three applications that don't follow this guidance, [00:13:00] which creates a recurring problem in our Sarbanes Oxley report.

And someone's going to say, why can't you just figure this out? We need to identify what is the cause of the problem and the root cause. The first might be because, well, new developers didn't know it was a requirement. Okay, that makes sense, but, uh, where is this tracked and assigned to them to get it done?

How many times are the developers reminded to get it done? What teams were assigned this responsibility, and did you train them, and did you document that training? And just because they got three alerts saying, please fill this evidence out, did they know how to do that job and how to submit the evidence? Or do we not actually give them the training they need to be successful?

So by figuring out what's going on, this didn't get reported. Why? Well, because the person didn't fill out the form. Why? Well, they didn't know where the form was. Why? Because we didn't include it in our training program. Why? Because we haven't updated our training program in three years, and the form came out two years ago.

Why? Okay, now we know what to go after. We don't yell at the person for not doing it. We go fix their training program. And that's the idea of the five why's. You can always figure out ways to get down to a [00:14:00] potential root cause that's gonna contribute to changing the end results instead of blaming people for doing what they thought they were supposed to do based on the information they had available.

See, when you find these root causes, you can create a way forward. Lean management has a concept of continuous improvement using a model of plan, do, check, act. And when you identify problems, test for a fix. If the fix isn't working, quickly do another fix. And that's why you should check quickly and study the results.

Be agile and implement solutions that work as soon as possible when you do that. You improve your success rate, and you create value for the organization. Remember, we live in a digital age with ever evolving threats, and our organization needs to constantly adapt. So find ways to measure the problem, such as threats to your business.

These could be IT threats, such as errors or mistakes. It could be cyber threats, when bad actors try to harm your systems with DDoS and other web application hacks. You might get telemetry showing that bad actors are pivoting. So now we need to pivot as well. For example, the bad actors stop sending phishing attacks in email and switch to [00:15:00] SMS messages.

What are you going to do about it? The bad actors use social engineering. What are you going to do about it? The bad actors switch to attacking MFA. What are you going to do about it? I just had that situation myself today when one of the executives said, Hey, I got this email with a QR code in it saying, Please scan this with your phone and follow it.

It's what's happening. The attackers haven't been able to get through to break into our PCs. They're pretty well armored up. We've got good layers of security. So now they said, Hey, let's divert this attack over to the cell phones. They may not be as well protected. So what am I going to do about it? I'm working on it.

So you need to have answers to these questions. Be proactive. Create a cybersecurity strategy that identifies where you're vulnerable, how you could stop these attacks before they happen. And if you can't automatically stop them, then how would you know that this attack is occurring in your organization?

What would you do to respond and recover to each of these potential attacks? When you flesh out your incident response plans and cyber strategy, you can create a cyber resilient organization. And you don't have to do this alone. [00:16:00] Ask for advice from your work colleagues, from your industry peers, from your vendors, and trust the third parties.

Everyone has an expertise in something, and when you tap into that, you can get smarter. You might see some new things coming out. For example, maybe there's a new tool that has AI or ML, which automates the manual process. Perhaps there's a zero trust security solution that shifts the way authentication and authorization is performed to greatly reduce your attack surface.

Maybe there's a future evolution in tools from Gen 2 to Gen 3 that have new capabilities that can really help. You won't know the answer to these questions unless you're on the lookout for better solutions. So... In closing, I want to emphasize the importance of measuring results in cybersecurity. It's not just a checkbox on a compliance list, it's a key to building a robust and adaptable security strategy.

Remember that cybersecurity is an ongoing journey and measurement is the compass that guides us. Stay vigilant, stay informed, and let's make cyberspace safer for all. Well, thank you again for joining me today. I hope this talk has shed some light on the critical role of measuring results in [00:17:00] cybersecurity.

As we wrap up today, I encourage you to reflect on how you can apply these principles to enhance your organization's security posture. I also kindly ask that you support our sponsor and check him out. They've got great white papers that are worth looking at. Finally, if you have any comments or questions, please go to CISOTradecraft.com where you can submit those. Follow us on LinkedIn if you're not doing so. Please subscribe on YouTube if you're not watching us on YouTube. That'll make sure you can go ahead and see where I come from,

different places around the world. By the way, different background as you might have noticed.

Greetings from Donegal, Ireland. We're happy to help you, give you some feedback on the type of content you want to hear more of. Until next time, I'm your host, G. Mark Hardy. Thank you again for tuning into CISO Tradecraft, and stay safe out there.