IT Matters Episode 40

Tue, Jun 16, 2026 2:17PM 35:04

SUMMARY KEYWORDS

cybersecurity, AI, multifactor authentication, threat intent, proactive disruption, reactive chaos, operational friction, enterprise-level budgets, legacy infrastructure, employee training, endpoint protection, managed services, vulnerability management, work-life balance, IT strategy

SPEAKERS

Keith Hawkey, Aaron Bock, Michael Irwin

A Aaron Bock 00:00

Welcome to the IT Matters podcast, hosted by Opkalla. We're an IT advisory firm that makes technology easy for your business. Our vendor-neutral technology advisors work directly with your team to assess technology needs and procure the best IT solutions for your organization. On this podcast, expect high-level expertise from our hosts, plus experience-driven perspective from the leading experts on topics like AI, cybersecurity, industry-focused IT solutions strategy, and more. Now let's get into today's discussion on what matters in IT.

K Keith Hawkey 00:35

And welcome back to the IT Matters podcast, hosted by Opkalla. At Opkalla, we help IT teams understand the busy marketplace of technology strategy and services with a data-driven approach. And on this podcast, we invite technology leaders to discuss the challenges facing the modern IT department. My name is Keith Hawkey, technology and podcast host of Opkalla, welcome to the IT Matters Podcast. Today's episode is going to be a little different, in a good way, because we're going to challenge some of the assumptions that have become pretty standard across the cyber security industry. We hear all the time, more spend, more tools, more complexity, but at the same time breaches aren't slowing down, and I think a lot of the technology leaders are starting to ask a simple question: Are we actually getting better or just getting busier? I'm joined today by Michael Irwin, CISO for Odyssey Logistics, who brings a perspective that I think cuts through a lot of that noise. Michael has spent time inside environments where the stakes are real and the constraints are real and the decisions aren't made in a vacuum, and he's not afraid to call out where he thinks the industry might be getting it wrong. And in this conversation, we're going to get into where cybersecurity investment might be missing the mark, and how to think about trade-offs between operational friction and real risk, and why it matters when you don't have enterprise-level budgets or resources. Michael, welcome to the IT Matters podcast.

M Michael Irwin 02:21

Thank you for having me.

K Keith Hawkey 02:24

So, there, okay? Before we begin, there's a little game that we play here to prime the session. Have you ever played Two Truths and a Lie?

M Michael Irwin 02:39

Two Truths and a Lie. I have. Yes,

K Keith Hawkey 02:41

the name is a little bit self-explanatory, so I'll.. these are cyber security. Well, actually, today it's a little less cyber security related, but it's tech related. Okay, and let's see if you can guess what the lie is out of these. So the number one AI powered holographic companions were introduced that sit on your desk, talk to you, and help with task, and even give you personal advice. This was introduced at the latest CES consumer electronics show this year. Number two, a startup has created a device that lets you upload your dreams and share them like videos with other people. Number three, robot vacuums are being designed with legs, so they can climb stairs and move between floors without human help. Let me know if you'd like me to repeat any of these.

M Michael Irwin 03:55

Well, I'd say in this day and age, anything AI related is perfectly feasible, that somebody's selling a product with it, right. So I don't want to go towards that one. Let's see, the I think I had seen something about some brain scan related imagery for dreams, or associating that, but that would normally be where I jump to. But I think I'll stick to the simple robot vacuum with legs. I have one, and it rolls around the house, and it's gotten smart, but legs it has not gotten yet.

K Keith Hawkey 04:24

Well, I'll have to say much to your amusement. Robots do have legs now. Our robot back of the vacuum apparently company named let's see Robo Rock unveiled devices like the Soros rover, featuring a wheel leg design that can actually climb and clean stairs, something traditional vacuums have never been able to do.

M Michael Irwin 04:52

Wheels and legs, though, that seems different, though. I wouldn't call wheels legs, there's a trick,

K Keith Hawkey 04:58

Maybe it was, maybe. A trick, and in addition, the gaming component company Razor has come out with an AI-powered holographic companion that it's actually very strange. It sits on your desk, and you can talk to it much like I guess an Alexa, but there's a visual component to it. It sits in like a little box, and you can adjust the looks, and it speaks to you. They are calling it Project Ava.

M Michael Irwin 05:34

Oh,

K Keith Hawkey 05:36

and to my knowledge, you might have knowledge that I don't. I don't think there's been major news of a startup that has a device that captures your dreams quite yet. However, honestly, I might just not be read in on that information yet. Well,

M Michael Irwin 05:53

no, I think I read something about like brain activity during dreaming and sleeping and tracking that, but certainly you're not going to have a video of what that dream was, I'm sure. So, no, that's interesting to hear.

K Keith Hawkey 06:05

Yeah, I'm sure. I'm sure it's coming, coming very soon. So, let's, you know, a lot of what this episode is about is challenging assumptions that are industry-wide within the cybersecurity landscape and industry, and it's gone through a tremendous amount of change over the last five years, last decade. Before we start, there, Michael, can you tell us a little bit about how did you get into it? How'd you get into cybersecurity? A little bit about your journey, and kind of where you got, how'd you get to where you are now?

M Michael Irwin 06:39

Sure, yeah, my really, my entire career path has been IT oriented, so I kind of started my career in managed service provider space, small, midsize consulting, or IT consulting, which I think is pretty common. Ultimately, at that time, was looking for an organization that I could really establish roots at, and something that I could see the long-term value of the work that I was doing, rather than kind of jumping into each fire, as I was kind of going customer to customer, and so that landed me at a media company in Washington, DC. So it's an ABC Seven affiliate, but also a media company that focused on political media, and I started with them kind of as a consultant, as somebody that was helping during the transition of a previous employee, and just was able to find an opportunity there, and that was something that I kind of grew through the help desk space, really, and more IT generalist at the beginning, but the track of help desk management leading into IT director kind of roles, and then really building a cybersecurity program at that organization within kind of the efficiencies that we found within the IT budget allowed us to really align those two things, I was there for about 12 years, and then ended up transitioning to another organization when I moved down to Charlotte, North Carolina. So, obviously, logistics were headquartered down here. I always, I always enjoyed the fact that cybersecurity is really industry agnostic. I was kind of curious about the idea of can I replicate the things that I did in this organization, and can I bring value with that to another, and that was kind of one of the things that I was looking for coming here. Obviously, Odyssey Logistics is a much larger organization, we're a global multi-multimodal logistics provider, and so we had a lot of presence kind of around the world, including in the United States. So, bigger teams, kind of bigger budget opportunities, kind of bigger scope of responsibility, and I think all of that was an interesting challenge, and what, what I found was much of my roadmap at an organization that was significantly smaller in a different industry really resonated in this one. Also, it added a lot of value, they had the similar challenges, they might have been at different stages of maturity, kind of in their technology journey, but really a lot of close alignment, and I think that was really eye opening to me, how a lot of those kind of simple things were able to land in such a good way. So that's kind of how I found myself here. I was brought in to build a security program, primarily, but early on was kind of given responsibility for the IT operations function as well.

K Keith Hawkey 08:54

And you've said the cybersecurity industry as a whole has failed, despite record spend and tooling, what do you mean by that? What, what are we measuring wrong exactly?

M Michael Irwin 09:06

Yes, man, at the end of the day, it's kind of the nature of the function, right? Cybersecurity is asymmetrical in general. We have to protect everything, and a bad actor has to find the one thing that we didn't protect. So, the odds are kind of set against you to begin with, but I think what you look at is, you have a lot of conversations around budget opportunity, team size, resource challenges, alert fatigue, like there's all these conversations about the challenges in the space where generally, and everyone would say they don't quite have enough cybersecurity budget right now, but generally speaking, cybersecurity budgets have grown annually. Most organizations are spending more than they ever have. Most organizations are building cybersecurity departments or functions that maybe lived inside of an IT operation function historically, and so the function is growing. There is no shortage of tools and services in the space that you can buy to solve your challenges, and so you're spending more, you have access to more technology, you have access. More resources, but breach incidents grow and grow, right? And the breaches you hear about aren't at every small mom and pop shop, but they are organizations that might be ISO 27,001 compliant. They might have a SOC two type two. So, if you have these mature organizations that are still experiencing breaches, and you assume that they likely have more adequate funding and resources to monitor what's going on, like, how does that reconcile, right? And I think a lot of it is, we're measuring effort, we're not measuring outcomes, we're still looking at kind of identity, is still that perimeter that we're dealing with, we're still looking at this castle concept in a lot of ways, we're dealing with a lot of legacy infrastructure, and I think a lot of that is that misalignment between cybersecurity and technology, much of the risk we deal with in this space lives in the legacy world, and if you have a technology roadmap that's not focusing on that, or you're not focusing on the kind of the housekeeping basics of stale accounts, or permissioning creep, or configuration problems, if you're not focusing there, but you're focusing on that new tool, you're likely missing the mark of where the majority of the trouble is.

K Keith Hawkey 11:03

Yeah, I think you're exactly right. Just wait for Gartner to come out with a new three or four letter acronym, and to start a buying cycle for said tooling, and a lot of that's laying on top of where the real risk lies, which is a lot of the maybe traditionally on on-prem infrastructure, some of the, some of the policies, the holy grails of organizations that new IT leaders don't really want to touch, because they're afraid to break certain things. You, you shared an experience where delaying MFA implementation led to a major incident. Can you walk us through that decision process, like what pressures were at play, and what you would do differently today? That's a kind of personal antidote we had spoken about, but I'm sure that would resonate with some of these cyber security leaders out there.

M Michael Irwin 12:00

Sure, I mean, this story is pretty straightforward, and hopefully for most people listening now, like this isn't still an active problem, because these controls have been needed for quite a long time. But earlier on, when I was dealing with this issue, what it boils down to is the usage of multifactor authentication alongside the usage of single sign on as a larger initiative, so getting away from distinct username and passwords for each service, more central identity management, ensuring that you have the right password policies, ensuring that you have multi factor authentication for everything, and the expansion of that effort is something I think a lot of organizations have are either actively going through today or have dealt with in the past, and during this time we were expanding on single sign on in that, in our, in that particular moment, there was a lot of friction relating to kind of user experience challenges, and so users had a particular understanding of what they wanted to do, what they thought was appropriate, what might impact their productivity, they had preferences on what tooling they got to use, or collaboration suites, and so it was a very kind of user experience oriented culture there, and they preventing any interruption to productivity culture, and so with that, we rolled out single sign on. We had documentation and training around how to enroll your MFA device, how to log in. That was all great. As we went to expand that functionality, we ran into a particular function, so VPN connectivity, that is something that traditionally didn't use multifactor authentication. You might be using simple username and passwords in order to integrate that functionality into that same single sign on system, maintaining the same ease of use that customer or that employees were experiencing. We weren't able to do that immediately, so it had some native functionality built in, some email based time codes, things like that, but didn't yet support the integration with our existing identity provider, and so what we chose to do was say rather than teach something else, rather than teach this new way of logging in, we're going to upgrade our firewall, we're going to upgrade that firmware, we're going to get that compatibility, and then we're going to roll out the way that we intended to, it's effectively looking for the perfect solution instead of progress, and in our case that decision, which really was just a delay of a few months, ultimately resulted in a large-scale incident that required quite a lot of kind of effort and financial resources to remediate, and ultimately was handled all right, but it's one of those things that you have to kind of go back and think, if I had prioritized differently, would this incident have happened? I'm a big proponent of not looking back with the same sort of perspective and saying, you know, there's something we did do that didn't allow an incident to happen. So, when you flip priorities, you can't just say that it wouldn't have happened that way. That benefit of hindsight, I think, doesn't favor people in this space very well, and so I think that's one that I try to look back at, is whether I'd make the same decision, and in my case, I think what the way I approach things today is more in a vacuum, it's more risk-focused, it's saying if the worst were to happen, what's the impact of this thing, this control that we're trying to. Impact really taking all of the other factors out of it and saying what's the what's the right thing to do first and then starting to look at how you can kind of modify that and fit into a larger strategy but when when you're looking at something purely from the angle of satisfaction I think you miss some of the the signs of higher level of urgency relative to the risk you're actually dealing with,

K Keith Hawkey 15:23

And those are those are great points, Michael. It actually goes, flows into the same vein of other points that you've argued that proactive disruption is much, much preferred than reactive chaos. I actually love that, that way of phrasing, proactive disruption is better than reactive chaos, which is much of what an IT or cyber security leader is dealing with today. A lot of them are reactive in the chaos, and some are, I think, are a little bit too slow to engage and make the case for that proactive disruption, whether it's password rotations, whether it's service accounts or restarting aging infrastructure. How do you decide when to accept that operational pain today versus the risk to tomorrow? Do you have a framework that you work off of?

M Michael Irwin 16:18

I wouldn't call it a framework necessarily, but I think a general principle is that if we're nervous to touch it, then we need to touch it, right? It gets this idea of if there's uncertainty like that, need that means we need to act, and ultimately, if we're going to take the hit, I'd rather take it on my own terms. So, if we have change management procedures and we're evaluating what the outcome might be if something bad happens, we understand what rollback procedures we have, or we can control it. We have the ability to fill in the gaps on that uncertainty more proactively, and so I would say it's less of a framework, so much as you are developing policies and program guidelines that force you to touch everything. You need to audit and evaluate the infrastructure you have. You need to do proactive patch management and vulnerability management on infrastructure that will require restarts, you need to be rotating passwords on service accounts that have maybe been around for a long time. You need infrastructure to do that more automatically. You need to be able to have those processes in place that require you to run into these problems, because ultimately, when an incident happens, the first thing they're going to do is have you restart, reset everything, every password in the organization. They might be accounts you don't know where they live, right? They're going to have you segment off areas of the network to avoid kind of lateral movement or sprawl. And if you don't know what infrastructure exists, you're going to have a hard time doing that. You need to install endpoint protection on anything you might be missing, or you need to give an incident response vendor access to see logging and material from all of your assets. If you don't know where those things are, you're going to have a hard time, right? So, this element of understanding what your entire environment looks like proactively, even if it makes you nervous, it's always going to be a better solution than waiting for the reactive event that then you have to act. I think most companies are generally weary of production impacts. They're weary of any business outcome that's negative, and I think part of this is just it's a messaging problem, a communication problem. If you're working with an executive team or a sales team or folks that are responsible for kind of customer experience, if they understand what that impact would look like in the worst of scenarios. It's better to understand why you're willing to kind of risk it a little bit more in the better ones. And obviously, the more you do this, the more you do this over time and track what you're doing, this problem starts going away. So, really, this issue at its core is a legacy problem, one that comes out of programs maybe aren't mature or haven't had that kind of formal focus, but it's a solvable one, where you stop dealing with that same level of concern.

K Keith Hawkey 18:46

And you've had exposure working in a multitude of industries, Michael, and I can imagine that the, the, you know, the receptive nature of making change, particularly disruptive change, can vary somewhat industry to industry. How does referring back to cybersecurity? You've worked in both media and logistics environments. How does the threat intent change based on industry, and how should defensive posture adjust accordingly?

M Michael Irwin 19:20

Yeah, I mean, threat intent changes everything, right? So, ultimately, your defenses should mirror what the attacker actually wants to achieve, and so you need to look at it. In my example, media, we generally focused on persistence and integrity issues, so we would deal with sophisticated actors that are trying to maintain control in your environment, perhaps for the purpose of modifying content that we're publishing, as an example, that is, by its nature, very quiet. It's something that isn't going to be the big noisy disruption that's obvious. And so, when you're looking at that, you need to protect that content, you need to detect subtle manipulations, and things you need to really focus on long-term access, things that are harder to detect, it. It really requires more visibility laterally across your infrastructure. When you look at logistics, I think it tends to be more financially motivated or disruption motivated, and so it's going to be louder. It's going to be more obvious. You might have an employee compromise of an account that you see negative effects of that same day. In media, you might have an employee compromise of an account that you see the effects of six months later, right, and so that nature of I can't remember what the exact statistic is right now, but there's a very lengthy multiple months period of time on average that it takes organizations to discover breaches, and a lot of that relates to what they're trying to actually achieve, and so when we think about logistics, ransomware disruption, the ability to recover, protect backups becomes a significantly more important control. I mean, all of them are relevant across the board, all the controls and the areas that you might deal with, but if you're dealing with priority, if you're dealing with budget limitation, it's important to understand kind of where the most important component is.

K Keith Hawkey 20:54

And you've also suggested that the majority of breaches stem from a narrow identity-driven attack path, which is the talk of today. If you walked into a billion-dollar organization tomorrow, what are three foundational controls that you would audit first?

M Michael Irwin 21:13

So that I would audit first is generally always going back to what causes an incident, what leads to a breach. So we're thinking about number one, if I'm going into an environment, there's an understanding of how well do they know their own environment. I've gone to organizations, or I've worked with groups before, that would say, "Oh yeah, we have our EDR solution deployed across all of our devices. Great, that's a great statement to hear. And you have a modern next-gen EDR, perfect. Now the question becomes, where's your asset inventory? Right, do you actually.. well, we don't have that, or there's uncertainty in that space. So, if you don't know the assets you're trying to protect, why are you certain that you've deployed them everywhere? That generally leads to a, at a minimum, 10, 20% gap in coverage at a lot of these locations. That ultimately leads to an incident. So, when you're thinking about what an organization might have what I would be auditing that awareness of their own environment, and really proving that awareness beyond just checking the box is critical. From there, once you know what your environment looks like, you again, you go back to where your problem is going to be. You're dealing with employee training and employee access issues. So, on training, that's obvious. You can do phishing simulations, you can have employee awareness training, you can measure how well they're behaving. That's all one component, but you can also look at, are they using single sign on? What does their password policy look like? Do they have MFA enabled for everyone? When you look at MFA these days, it's not as straightforward as a simple code that you need to present, but rather, are you protecting sessions? Do you have proactive awareness of session behavior that's an anomaly, something that might signal a token theft in an environment. There's a lot of organizations that are checking all the right boxes, but they, un, they, they kind of miss the understanding of the underlying ways that bad actors are using these accounts, and they're bypassing them, and so it's really a moving target that we have to hit. But outside of that, you look at endpoint protection, right? So, I, I tend to not be as infrastructure focused at the beginning. I'm much more user focused, much more user device focused. So, even thinking about things like segmentation, I think there's a lot more value in segmenting a user population from one another than there is segmenting, say, resources in the data center. One might be more important. A lot of people talk about what the crown jewels are, the most important assets, and that's all true, but access to those things generally starts with that user device. It's going to be the email they click on, the malware they download on a computer, and where they can get from that device laterally is what that bad actor is going to be following. So, really sticking to the common causes of incidents is what's going to move that the needle, particularly in ROI, and is really achievable with low investment. I mean, it's a people and process problem more than it is a technology problem. So small, mid-sized businesses that are trying to kind of keep up with this changing world in this space, that's an area that you can really add a lot of value for limited budgets.

K Keith Hawkey 23:57

Yeah, and following up with some of the security tooling that you're referencing between EDR asset inventory, you also suggested that much of the industry messaging is geared toward the enterprise space, not the mid market. Like, what's.. I mean, you've.. I'm sure you've listened to dozens and dozens, and maybe even hundreds of cybersecurity tooling pitches in your career. What, what cybersecurity advice sounds impressive, but it's really irrelevant for most mid-size organizations.

M Michael Irwin 24:34

So, I think anything that is pitching you at this kind of re-architecting of the way your business operates as this prerequisite is always always kind of makes your alarm bells goes up. Obviously, in this day and age, AI is a big center of that, right? There's a lot of assumptions that are being made with the value that certain tools in that space might be able to provide. Another big one is that there are a plethora of products that will say we. Will give you full visibility into your network. We'll show you all of the traffic, we'll inspect all the packets, we'll show you all the vulnerabilities, we'll give you all this information. And that sounds great if you have a large team to actually act on those recommendations, but if you don't, and you're expected to provide them, and you have a PowerPoint presentation with a bunch of green, yellow, and red check boxes that you're trying to kind of show posture to another group, it's not really impressive if you can't act on it, right? And so it's funny, one of the thoughts I have, and kind of hard to say where the right answer is, but if you have 100 vulnerabilities and you can't solve them all, like, do you want to even know, right? Is it valuable to even know a vulnerability exists if you can't remediate it. It's kind of like, did a tree really fall in the woods if you weren't there to hear it, right? It's that kind of idea.

K Keith Hawkey 25:45

Yeah.

M Michael Irwin 25:46

And so I think, because of that, what especially small or mid-sized companies need is focus. They need focus on what is actually being compromised. They need focus on things that small changes that make the most large scale value. So, if we're talking about upgrading or patching something, something that affects multiple devices, not one. You're really looking for something that you can actually act on. So, even in my own space, an area I always look for is what organizations are providing a tool, and they also have a managed service component. CrowdStrike, as an example, as an EDR solution, has a managed services component to their licensing that you can provide that's actually doing some of the work for you. Other managed socks service providers might do the same thing, right. So, there's different players in that space that say we won't only tell you when there's a problem or there's a risk, but we will help you solve them, or we will help you weed out the noise. Those are things where you have a lot more value, and I think oftentimes presentations or conferences that are geared towards larger organizations, generally because they have larger budgets to pay for the products that they're being pitched. Those sort of things often assume a level of resource, a level of maturity, a level of documentation, a level of things that have already been achieved in order to be successful, but they kind of gloss over that at times, and so it's, it's difficult to look back and say, oh yeah, it's great, you're referencing a problem that we know exists, this is a risk we're concerned about, your tool sounds great, but I have 10 other things I need to do before I can even get there, right? And I think that's where that message gets lost on smaller audiences.

K Keith Hawkey 27:22

Yeah, I couldn't tell you how many, how many demos that I'm on. It feels like weekly that the whatever name your cybersecurity vendors is requesting the client completely re-architect their their network design and I give kudos to some of these AI advancements, like, like you said, that really, where these cybersecurity vendors make their money and differentiate themselves is the services that they attach to the tooling, because I have a lot of, I have a lot of clients, quite frankly, that they just can't handle the alerts that the mid-market IT teams are lean, and more information really isn't bliss. Yes, it actually just causes them more headache and heartburn because they can't get to everything. So, you know, having there are some innovations in the AI agent space that we are seeing with cybersecurity that hopefully can help remedy some of the log ingest some of the tasks, some of the especially the level one, level two tasks that don't require network changes, don't require like fundamental changes to the existing ecosystem that can help, hopefully, save the day to some extent with that increased visibility.

M Michael Irwin 28:46

Well, it's interesting, though, because I mean, I think one of the challenges that we have in the space is cybersecurity. Obviously, there's stress, there's burnout. I think what people don't talk about enough is there's a lot of imposter syndrome, right? There's a lot of people that they're in a role, they're responsible for something that they don't know they don't necessarily have confidence that they know what the right answer is, and you look at that in the example of AI. Let's say AI as a concept is now talked about everywhere, people are trying to bring it in, your board, your leadership wants to bring this technology in, you're tasked with protecting it, and this is something that is new within the last year or two, right, depending, I mean, not new conceptually, but new as far as kind of public favor goes, and so you're now tasked with not only understanding this thing that is new and everybody's trying to learn opportunities for, but also understand and articulate the risks involved with it, the potential gotchas, the configuration mismanagement, the how to do that in a safe way, and like you need to do all of that at the same time, and I think when you look at that concept, and you say I have alerts that are generated problems that are generated from a tool, I have some AI integrated function of that, that is now telling me what to do, it's maybe translating something, and that's where I've seen a lot of success is taking a technical alert and translating into. Simpler language, because many of our teams are lower or mid-career people. They may be focused on their past experiences, they don't have the technical knowledge of some of the stuff they have to learn. And so that balance of AI is helping you move faster, maybe it's telling you how to remediate it. To what degree, or are we there yet, that we trust the answer it's providing, right? Especially with a team that can't necessarily vet that, or is missing some of that, and I think that leads to hesitancy, and so I think when you run into that space, is the idea that there's certainly opportunity, without a doubt, there's certainly value that these sort of approaches have for organizations, but when you are using it as a fix for what is an underskilled or under-resourced team, I think there's often this fork in the road, or this kind of mid intersection point, where they come back together, and you're going to kind of run into that same problem. And I think that's the piece that, when we talk about people, process, and technology, what I often find is, in this, at least in the sense of AI, is that it's technology in search of a problem. Traditionally, we've looked at technology as we have a problem, we have a process, and we're looking for technology to be something that will help with scale, it'll help with efficiency, it'll add value that way, but you're starting from the focus of a problem. I think when you go back to that and you think about in the cybersecurity space, a focus on people and process, you focus on administrative housekeeping, you focus on best practice and kind of cleaning up what you have, and then you identify something that has too much volume for your small team to handle, that becomes a great use case to leverage that AI or that kind of optimization technology into the mix to make you better, but at that point you're coming from a point of awareness and strength, you're not trying to fill a lack of awareness with it. Right, I think that's a distinction that often will drive whether or not you're successful in using it.

K Keith Hawkey 31:47

I feel like we could talk about this for hours, Michael. I really appreciate the antidotes and the conversation that we had today, challenging some of the assumptions in the, in the cybersecurity industry. Just, just leaving here, if you were going to have a message to a let's say a green behind the ears cyber security, formerly it getting into the cyber security world leader, what what message, if it could fit on a billboard, would would you share with with this individual?

M Michael Irwin 32:24

I think the main story is that you will be tasked with solving problems that you didn't create, and that's the nature of the business. And so, what that means is there might be more than you can handle, but you can continue focusing in a methodical way, and you can always make progress, right, whether it's small budgets or big budgets. If you have an understanding of everything that needs to be done, and you prioritize and really align with the business based on where they are kind of financially or economically, you'll be able to continue making progress, and what you really find is a lot more success with that same business seeking funding if you are understanding of the financial position they're in, so if you're in a lean budget year, that's the time to look for high ROI people in process work, right? If you're in a higher budget year, something that has a little bit more capacity for new tooling, maybe that's a good opportunity to look for those high value but higher dollar investments that you have. So not being able to do the high dollar investment in a lean year doesn't mean that you can't be successful, it means that you need to be aligning to what the business needs in that moment, and there's always work that can be done, and I think when you look here, what really moves the needle in protecting against incidents is just that, and the only other thing, because I think it's important, is don't overlook culture, right, because when you think about people, when you're talking about AI, when you're thinking about this work, the inevitable bad days that you'll have, focusing on positive culture and work-life balance and really supporting the people on your team moves the needle more than anything else.

K Keith Hawkey 33:47

Yeah, very well said, Michael. How can you, how can our listeners get in touch with you?

M Michael Irwin 33:54

So I'm available on LinkedIn, so you can search and find me there. I generally accept invites from whoever, whoever asks, so I'm not, not particularly limiting on that front, but I'm pretty active in the Charlotte CISO community, so I'm a lot of events in this space, some of the Gartner Apex Assembly things, there's various things that are going on, so I tend to be in those spaces, but yeah, always reach out, and I'm happy to chat, I do a lot of mentoring for individuals, particularly coming from kind of IT backgrounds, or looking to get into cybersecurity, so I'm always open to chat if anybody wanted to speak about anything.

K Keith Hawkey 34:25

We'll make sure to include that information in the show notes. Michael, thank you immensely for joining the IT Matters podcast. Thank you. We will catch you guys next time.

M Michael Irwin 34:35

All right, thanks.

A Aaron Bock 34:37

Thank you for listening, and we appreciate you tuning into the IT Matters Podcast. For support assessing your technology needs, book a call with one of our technology advisors at O P K A L L A.com. That's opkalla.com. If you found this episode helpful, please share the podcast with someone who would get value from it, and leave us a review on Apple Podcasts or on Spotify. Thank you for listening, and have a great day.