IT Matters Episode 39

Tue, Jun 02, 2026 3:37PM 30:49

SUMMARY KEYWORDS

Cybersecurity, compliance, CMMC, NIST 801 71, IT strategy, AI in defense, security culture, cybersecurity podcast, ransomware, multi-factor authentication, third-party verification, cybersecurity frameworks, IT advisory, technology solutions.

SPEAKERS

Nathanael Dick, Keith Hawkey, Aaron Bock

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** 00:36

Welcome 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. On this podcast, we invite technology leaders to discuss the challenges facing the modern IT department. My name is Keith Hawkeye, Technology Advisor at Opkalla, and I am pleased to announce we are joined by Nathanael Dick, who currently serves as the director of cyber security and governance at Steel Fab. Nathanael brings a really practical perspective to security, someone who's not just thinking about frameworks and compliance and theory, but actually using them to drive stronger, a more resilient organizations. He's got a background that spans cyber security leadership compliance strategy, especially in the areas of CMMC, which we'll dive in today. He's also deeply involved in the broader security community, even co-hosting for a stint his own cybersecurity podcast, and regularly is a speaker on many subjects. Cybersecurity in this conversation, we're going to get into how security leaders can rethink compliance, not just a checkbox exercise, but as a lever for maturity. How AI is both the threat landscape and in defense strategies, and what it actually takes to build a security culture that sticks inside an organization. Nathanael, welcome to the IT Matters podcast.

N Nathanael Dick 02:19

It's great to be on, Keith. Looking forward to it.

K Keith Hawkey 02:23

But as per usual, we are going to start with a little game, if you don't mind, Two Truths and a Lie, and this is cybersecurity focused. Do you know how to play Two Truths and a Lie?

N Nathanael Dick 02:38

Actually, don't.

K Keith Hawkey 02:40

All right, so I'm going to read off three. They're sort of news events, and two of them are true, and one of them is completely made up. And I want to see if you can guess the falsehood. That's the idea. All right, so two truths and a lie. Are we ready?

N Nathanael Dick 03:01

Ready.

K Keith Hawkey 03:03

Okay, so number one, a Fortune 500 company experienced a breach that was definitively tracked to a compromised smart refrigerator on its corporate network. I'm Number two, security researchers demonstrated it's possible to run a functional Linux environment inside a PDF file by abusing the PDF format scripting and rendering capabilities, highlighting just how flexible and risky, widely trusted file formats can be

N Nathanael Dick 03:46

Very good.

K Keith Hawkey 03:46

and and number three, a ransomware strain known as Volk Locker was discovered with a critical flaw. The attackers accidentally included the decryption key within the malware itself, allowing victims and researchers to recover files without paying a ransom.

N Nathanael Dick 04:06

I'm going to go with number one as the lie.

K Keith Hawkey 04:12

You are correct, I there are no, at least reported instances of Fortune 500 or Fortune, any any 100 companies having their network breached by a smart refrigerator on the corporate network, because that would be entirely embarrassing, but I actually think it's coming. Good idea, Nathanael.

N Nathanael Dick 04:32

Yeah.

K Keith Hawkey 04:33

it's just hasn't.. it's going to be one of our truths in the next year, is what I'm guessing.

N Nathanael Dick 04:38

Well, we had the target breach, which was an HVAC, so it's kind of waiting for that one, but refrigerator. I was like, okay, yeah, hopefully they put it on the guest Wi-Fi.

K Keith Hawkey 04:50

Yeah, exactly. So let's talk that, Nathanael, you have a breadth of cybersecurity experience, I'd. Love to learn a little bit about how you got into the industry. What inspired you to go down this path? Some of your background, can you kind of introduce us to Nathanael's kind of path to where he is today?

N Nathanael Dick 05:11

Yeah, so it started back in, I guess this could start as a teenager building a business with my brother, and through that process learned a lot about business and how to sell things online, and a little bit about scammers too, and then went to college and earned my Bachelor's of Science in Computer Science, and then started in IT for a defense company, and during that time there really got a lot of experience, had some really great mentors there that helped me learn a lot, and so I just was taking in a lot of information and really grew to love a lot of areas of it, and then I started to lead that IT department and got into a lot more with and we'll probably talk about this later on the importance of how defense companies need to meet federal compliance and then that kind of led me into the compliance space and along that path also the cybersecurity space so just started to really develop a passion for securing environments and the importance of using frameworks and third-party frameworks and best practices to apply those principles, and somebody that didn't know a lot of that, doing a lot of learning, and what really helped along the way was those frameworks to understand here are the best practices to apply to a company's security posture.

K Keith Hawkey 06:54

I know that there's one point in which kind of on your journey that you were handed a regulation to handle.

N Nathanael Dick 07:03

Yeah.

K Keith Hawkey 07:03

So tell us a little bit more about about that experience.

N Nathanael Dick 07:09

Yeah, so we were a defense company in Grand Rapids, Michigan, and remember my boss one time we were kind of working through the NIST 800-171 compliance, which is NIST stands for National Institutes of Standards, and it's a publication arm of the government that publishes best practices for the government, and NIST 800-171 is a compliance requirement that they started to enforce for companies that do business with the Department of Defense, so back sometime in 2017 we were working through that process, and I remember one day my boss at the time at this company, he was a great guy, great mentor, and we looked up to him, and he, he handed me this regulation, or said, "Go ahead and read this, and you'll probably fall asleep, and I took that, as you know, kind of an opportunity, and ended up just really actually not falling asleep, but just kind of engaging with the document, and in really having fun with it, and I started to see a lot of commonalities as we worked through understanding the different specific guidelines and legal language in the framework, and so that really was a, was a game changer in, in how not only the company looked at compliance, but I was able to develop a lot of informational learning myself, so that was a great opportunity, and also it just kind of developed my, my passion for, for frameworks and cyber security too.

K Keith Hawkey 08:54

A lot of new cyber security leaders view compliance as a burden and as a big pain, and I just find it, it's interesting, compelling. How you, you took this piece of regulation, you took this assignment, and you were engrossing material, and didn't think of it as, as a checkbox, but how can, how are you going to improve security maturity at your organization, that it, it is something to embrace and live by as a security professional. And where do you see organizations get this wrong and treat CMMC like a checkbox instead of a real transformation?

N Nathanael Dick 09:38

I think it is partly a mindset shift, because we start to look at compliance as kind of the bad boy in the room, and something to blame your problems on, because we don't want to engage with the compliance framework and find a business solution, so I'm a big believer that cybersecurity compliance. It needs to help the business, it can't pull back the business. So, going back to my experience in business, and also have my MBA, I think that's vital to understand we need to encourage the innovation and success of the business, and that's the first goal. So, compliance and security have to support that, and so I think it's that mindset shift. Once you kind of get over that mindset shift, stop blaming security and start to enable the business. Some practical ways that can just kind of do that is instead of being saying, hey, this needs to be this password policy needs to be this way, maybe there's some creative ways that can be just as secure, even more secure. You get your users to engage with why you have it this way, and then they can kind of have not input, but they can kind of help guide that process of innovation, so you're not, you're not just being the police and saying it must be this way, you're kind of working with the business, different stakeholders in the business, making sure they can still do their work and being compliant, so there's a lot of ways to solve compliance, and a lot of people think it's just one way, but if you, you're careful and you engage your stakeholders, you can really have success, not only in being compliant, but making it so that people come back to you and ask you these questions and keep your business safe.

K Keith Hawkey 11:38

There is a significant compliance benchmark that's coming up in October of this year with CMMC and lots of organizations are behind the eight ball, as I've discovered in my day job, and are scrambling to make ends meet to reach this compliance, you know, there's different levels of compliance requirements, so they can bid on those juicy government contracts and agency contracts. Maybe you could just, you've been on this journey, could you kind of delineate what are the different diff, what are the differences between the different levels of CMMC? I know there's a level one to what house, if you're, if you're just starting down this journey, and if you are starting now, you are way behind. Let's, let's hope that you're made some progress. Yeah, it's yeah. How should someone that's been assigned this journey kind of think of the different levels and sure what's good for them?

N Nathanael Dick 12:37

So, there's three levels, and I'll take a step back. So, first of all, in context, the problem the government faced back in 2000 and even in the 90s was we were losing our secrets, so the F 35 fighter jet was stolen by the Chinese, there was a lot of other pretty major secrets stolen, and so they had to get their handle on all this data being lost, so they developed what the NIST 801 71 standard, and in 2010 there's also executive order by President Obama to kind of consolidate the different data types that the government had, and it was fine storing, in the most part, classified data, which think of like movies where you see these big rooms and all this very secret stuff, but the problem was all this data that was not classified. When taken together, these spies and these organizations could actually develop some pretty major informational data points that could lead to these secrets being stolen, so the government realized that, and then try to consolidate that into what was called control and classified information, and then over the years regulation was enforced on businesses that handle this control and classified information, and they had to comply with 110 cybersecurity requirements for the NIST 801 71 standard, but nobody really was doing that, so they were saying they did in general, obviously there was some exceptions, but nobody was really taking it seriously, because there was really no skin in the game. The government was saying just do it, and we may check you, but not a lot of people really checked. So then they realized how we need to start to validate this and have a way to make sure if you say you're compliant, you have all these under 10 requirements, you actually are compliant, and that was what caused the cybersecurity maturity model certification to go into effect, the whole basically the whole thing, the whole process. Processes, you have an auditor come out and verify you are meeting these 110 requirements. That's it. That's really in a nutshell what CMMC is. Now, then you kind of get a little bit more in depth. You do have CMMC level one, so that's a base controls, so it's going to have a lot smaller subset of controls, and actually a third party verification is not required, so that's the MMC level one, and this is for data that's not even CUI, so this is what's called federal contract information, so very non-technical data and it doesn't even meet the controlled unclassified information, so if you do do any kind of what we call controlled technical information, so code drawings, things like that, you're you're likely dealing with controlled technical information, and then you're dealing with CMMC level two, CMMC level two is those 110 cybersecurity requirements that align with the NIST 801 71 framework, and so that's where organizations largely need to get audited by what's called a c3 PAO, or third party certified assessor, and that's the main bucket that organizations are going to fall into. We're not going to see a lot of organizations fall into the next level, which is CMMC level three. Those are more critical programs that maybe space satellites, things like that. I don't even know, but critical sensitive programs that would need that CMC level three.

K Keith Hawkey 16:51

Why has this been delayed over and over and over? Do you like.. I remember five years ago this was,

N Nathanael Dick 16:59

Yeah.

K Keith Hawkey 17:00

This was coming, and it was delayed multiple times. Do you know, do you have any insight, like why they delayed these ramifications and the seriousness of this? I mean, it seemed like it would have been urgent,

N Nathanael Dick 17:15

Yeah.

K Keith Hawkey 17:15

many years ago, but

N Nathanael Dick 17:16

You would think, right? But it's something I've been frustrated, kind of in general, just in industry, is kind of at least there's us fans of CMMC, which I consider myself a fan.

K Keith Hawkey 17:29

There you go.

N Nathanael Dick 17:29

I'm getting a little bit frustrated because it has gone through a lot of what I call industry criticism, and it's, it's understandable. I think a lot of it has to do with maybe some of the ways it was rolled out originally, so there was a CMMC phase or version one, and that was a little bit more maybe rigorous, you could call, or confusing. There was actually five levels in that, but only three counted, so it's kind of confusing, and I kind of wonder if a lot of that failed first version of CMMC was largely due to just the confusion around the communication, because I remember people explaining it, and it was like, why do we have level two, and you don't really need to do level two, but you have level three, and you need a level, so it was very kind of in this confusing space, so they made a lot of good changes, and they did listen to industry, so they did get that right, and when they came out with what we call now version two of CMMC, it was had a lot of good industry insight and feedback, and so I think they came out with a good product, but it did take the speed of a turtle to get here, for sure.

K Keith Hawkey 18:48

Yeah, really, is CMMC level one just kind of the training realm? I mean, it sounds like the one that really matters for 95% of organizations that are engaging with CUI and classified information are going to need level two. Are there organizations that it's just a good training exercise for level one? I mean, I doesn't seem like that would be a requirement. Yeah, more of like getting you started.

N Nathanael Dick 19:19

Well, you know, there's CMMC level one, there's some, there's some tough controls, um, some physical access controls, and some others too. So, there's some things there that do take some investment and time to at least document and show what you're doing. I think, but it's a very baseline level, and hopefully you've been kind of doing that already, so if you're not at CMC level one, even you have a lot of work to do, but for the most part, you are going to see most companies going to be at least that handle CUI for sure, if they handle CUI. Going to be at level two, so yeah, there's definitely going to be quite a few that are level one. In fact, you can do a search on sam.gov which has a list of all the contracts, and kind of look at that. What is even now a requirement for level one? So there's even some CMMC level one and two out on sam.gov so we're actually in the first phase that started November of 2025 all the way to the next phase, which starts this year, so people were saying, "Oh, this is going to be the harder phase. Well, it probably will be, but we're already starting to see some of these requirements pushed out already, so it's really important to be aware of that and be ready as soon as you can.

K Keith Hawkey 20:50

Was there a point when you were, you were approaching your level two certification where you thought we are not as ready as we thought we were, were there any gotchas, any trip ups that someone cybersecurity leader that is going down this journey should be cognizant of, should be thinking of anything like that in your story.

N Nathanael Dick 21:18

Well, thankful we had a great team, so it took IT full IT security effort. My boss, Sandra Clay, was awesome, and the whole IT team, we really kind of worked together really well, and we had a really successful process down, and so that was good from what I've seen in industry, and just kind of the talking a lot of colleagues is probably the biggest challenge is figuring out who's going to kind of own the CMMC space, and then after that is like making sure you are scoping kind of your environment correctly, and that's probably the biggest gotcha, where you may not really understand what you said you were doing, and that could be a cause for an audit going awry, or you see a lot of where a consulting company will kind of generate a lot of the documentation and policies, and then you may be reading it, and you're like, okay, well, you know, are we really doing this? So I think that's the kind of gotchas in industry is make sure if you have enough policy, make sure you're actually doing it, and make sure you have a lot of review kind of built into all your documentation. Probably 80 to 90% of CMMC is documentation, whether that's policy configuration or just the continual maintenance and review process of CNOC, the last 10% is just good cyber security controls, and you, so that's kind of the main uplift. Yeah, there's definitely significant investment in some of these controls, like multi-factor authentication, but not really. I mean, a lot of that is just already pre-built into, like, Microsoft, for example. So it, the real work is the documentation and making sure it ties back to your, your configuration, your controls, so

K Keith Hawkey 23:42

With those third party, because, because I work with them, I work with companies that do this, can provide a lot of the documentation and offload that burden from an IT team, but it sounds like the way you made that this appear is that sometimes you can get into trouble to some extent when a third party's supplying a lot of your, your quote unquote policy that your company abides by, and their interpretation of how your organization is abiding by this policy may be very different than someone internally that knows how that organization is abiding by certain policies, and then when the audit comes around, it might, you might be in a sticky situation if you lean too much on a third party that's going to do a lot, a lot of this work. Is that kind of what, what you're getting at?

N Nathanael Dick 24:34

Yeah, we have some great MSPs we work with too, and I think the main piece is if you use an MSP, that's great. Just make sure you know what they're telling you, and they're advising you, and make sure that you understand it yourself, or somebody at your company. Maybe I always recommend companies choose a CMMC main person. They don't have to be the expert. Everything, but they should kind of know a little bit about the regulation, and then they should definitely know your policies backwards and forwards, and then that can be your really main point person. So, even if the consultant creates a lot of the documentation, that's great. I love some of the consultants out there that that do that, and they have some great products, and I actually recommend you kind of use some of their products, but make sure you know what they say and what they recommend, so as it applies to your environment. When the auditor comes, you can be the one to answer that, and that's going to help when you make upgrades to your system. Say you need to, you need to make an upgrade if you aren't aware of what your policy says, and you just make the upgrade, that could be a violation of the policy, or it could impact you long term and make you get out of compliance. See, really, it's really critical. We, we obviously went through a steel fab, steel fat went was one of the first fabricators to go through a level two audit, and we're now, we're in the maintaining phase, and that's just as important as a, as getting this, the certification is maintaining it, and making sure you're aligning with it. I hear a lot of people say, okay, once we have it, you know, we just can kind of turn off the, or we can kind of let go of the consultant now and figure it out, but you got it. There's a lot of maintenance to be done. There's a lot of things that have to be done on a weekly, daily basis just to maintain that certification.

K Keith Hawkey 26:38

That's, that's, that's so valuable to, to hear, Nathanael. We're running. I feel like we're just scratching the surface, but we're running up on time on the podcast, so we'll have to have you back to follow up, maybe even after these deadlines actually take place in October for CMMC level two. One thing that we like to do at the end of the IT Matters podcast is, well, actually make this close to home. We both live in Charlotte, so let's say you've got, you know, everyone uses I 77 to go up and down Charlotte. If you could rent out a billboard on I 77 that all these IT leaders and Charlotte could see about something that you think is missed in either IT or cyber security or a message or something that you think is kind of the unsung virtue in the industry, what would you want to kind of, in short form, what would you put on a billboard that, if every IT leader could see that you think is missing?

N Nathanael Dick 27:52

I think it's a great question, and I think what

K Keith Hawkey 27:55

I know, I sprung that on you.

N Nathanael Dick 27:58

What I would say is keeping aware is so critical, like I just think about some of the people that come up to me, my friends, or even coworkers, and they, what always is so critical to stop on the bad guys is to be aware, and maybe I would put, you know, stop and think. I think those would be the two things, and in that would probably solve most of, in stop most cyber incidents, if people stop and thought before doing whatever, whether it's clicking something or maybe responding to somebody, or in any type of action, in it really comes down to, we stress this a lot at our company, is it's a team effort, and it's not just me and my office, and I'm, I've got all the cool cyber gadgets. It's really having a team, and it's not just the IT team, it's the entire company, and that's what keeps us safe and cyber safe.

K Keith Hawkey 29:19

Stay cyber safe. Stop and think from none other than the great Nathanael Dick. Thank you for taking a little time to join the IT Matters podcast. Nathanael, where can our listeners find you? They have any questions if they're beginning this journey down CMMC. What's a good place for them to talk to Nathanael.

N Nathanael Dick 29:42

Yeah, so I love just engaging on LinkedIn a lot, so you can find me on LinkedIn. Feel free to message. Always interested in hearing other people's CMMC stories and cybersecurity stories, so love to continue to just collaborate, um. And I always enjoy hearing other people's stories.

K Keith Hawkey 30:04

Perfect, we'll put the Nathanael's LinkedIn information and the show notes, and with that we are done today, and we'll catch you on the Not the next IT Matters podcast. Thanks for listening, and we'll talk to you soon.

A Aaron Bock 30:22

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 oppallo.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.