#124 - Simple, Easy, & Cheap Cybersecurity Measures (with Brent Deterding)

[00:00:00]

[00:00:11] **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. My name is G Mark Hardy, and today I'm pleased to have Brett Deterding on our show. Welcome, Brett.

[00:00:27] **Brent Deterding:** Hey, thanks for having me.

[00:00:29] **G Mark Hardy:** And we're going to talk about a number of things, but we're going to be looking at security, cyber insurance, risk, a number of topics are going to be really important to CISOs.

So as a reminder to you, if you're watching us on YouTube, great. Please. Follow us, click follow. Good. Let's get our subscriber list up because the more we get, the more people we can reach and we get better control of the show. If you're listening to us on audio, come on over to the video and vice versa.

Also, if you follow us on LinkedIn, you'll find out at CISO Tradecraft we've got a lot more than just the episodes that we put out here. [00:01:00] We've got a steady stream of really, really good information. So with that ad out of the way let's get rolling. So one of the gentlemen I got a chance to know over the years is Bruce Schneier, and Bruce had said a number of years ago, well, he said a lot of things, but a fundamental rule of cybersecurity is complexity is the enemy of security.

Cause anytime you add a new product or new feature, well you're going to introduce new risks. For example, if you add a new website that takes in user input, then there's probably some unknown way the website could be hacked and someone could steal all that data. Yet at the same time, you have to constantly add new features and products to stay profitable and to compete against your competition.

So cyber has caught an ever-present battle. We have to ensure revenue protection. And we also have to enable the business. So today, let's go back to

the basics. Let's say the small companies just asked you to be the company's first virtual CISO. And since it's a smaller company, there's really never been anyone around to look at cybersecurity within the company.

So you're starting from scratch, and now you look around and [00:02:00] you see the following service offerings. Everybody's using a Windows laptop to do their work. Okay, and they're using Microsoft Office 365 for business productivity using Outlook for email, teams for video conferencing, documents are written in word, files are shared with OneDrive or SharePoint.

Pretty standard sales billing is done with Salesforce, accounting with Intuit QuickBooks, HR functions with Workday and let's add one more component Documents which require signatures will leverage DocuSign. Now, this is probably one of the most common baseline setups that you'd find in corporate America today.

Now, thank for a moment. How would you protect this organization? You'd start by ensuring revenue protection. Here's an important point. Remember, cybersecurity is all about understanding, managing, and mitigating the risk of your critical data. It could be disclosed, which is confidentiality, could be altered which is [00:03:00] integrity, or denied which is your availability.

Now, at the beginning, you need to start with strong authentication and access control, and this is why I hear the term MFA or multifactor authentication so often. Here's a pro tip, not all MFA is the same. There are multifactor authentication methods that are phishable, and of course those aren't as good as ones that are not phishable.

You want good mfa? So look for MFA that supports the web authentication api, which is also known as WebAuthn, if I'm pronouncing that correct, or FIDO2 passwordless authentication. Now, we did a deep dive on passwords and authentication in episode 74, so please check that out if you're looking for more detail.

Now here's a simple example of an effective implementation. Your organization uses Microsoft Azure Active Directory, and it ensures that users will log in from a trusted device, and the organization owns the device like a laptop, and the user provides a password to the account. Use hardware token, let's say, YubiKey to log into [00:04:00] every service.

And in this simple method of verifying identity based on a user device, a password, and a token does go a long way to keep external actors from

accessing your sensitive applications, which would be the key to confidentiality. Now that we've done the first step of protecting access to important web applications, we need to think about keeping our laptops secure.

And the first way laptops are going to be attacked is when employees will click phishing emails, and those could contain harmful links or attachments. So we need an email security solution. Microsoft offers Exchange Online protection or E O P for about a dollar per user per month, but it could go with a third party like Proofpoint or Abnormal Security.

Next, we're going to need something that monitors the laptop directly. So they can identify if malware might have been downloaded from a website via web browser. And we often see organizations running endpoint detection and response EDR software in combination with antivirus AV, we, we know these acronyms, but I'm including them [00:05:00] because you're always supposed to define your acronym at first use.

And examples of this could be Microsoft Defender or CrowdStrike. But be careful. Don't just check the box with a free antivirus software because when you're trying to secure your organization when it comes to free software, sometimes you get what you pay for. And as a security professional, it may not be worth both the corporate risk as well as your career risk.

Well, now that we've got the basics of MFA, EDR, AV, and email security, there's one more must have tool that we think is really important. The fifth essential tool is a good patch and vulnerability management solution. Essentially, want to make sure that any of the devices your company runs are both patched and configured securely.

And many companies have used tools such as Nessus or Qualys, or Rapid7 for years. But today I'm going to mention another product you might consider called Microsoft Defender Vulnerability Management. And this new tool for Microsoft allows you to see a consolidated asset inventory of [00:06:00] applications, browser extensions, and certificates. Allows you to block vulnerable versions of applications and monitor compliance against industry benchmarks such as the center internet security critical control, so the CIS top 20, which are now down to 18.

You can even manage remediation activities, and this means you can easily identify laptops that have vulnerable versions of Google Chrome or warn or force users to patch their laptops with uncertain timeframes, there's a lot more

powerful capability there than just knowing the device is vulnerable and not taking action.

Now we can do something about it. So now that we've achieved a simple set of protection tools, what's next? And the truth is it should become a business decision on where to focus next. And here, five helpful options you should consider strongly as potential next steps. Number one, risk assessments. Risk assessments help you identify the likelihood of attacks, the impact they'll create, and the remediation steps that your organization has agreed [00:07:00] to follow.

And by following this approach, you can create processes that will align with security guidance from standards such as ISO 27001, which is great from a compliance perspective. Number two would be incident response plans. And you know, at some point there's likely going to be an incident. Well create some helpful response plans in advance.

Think of scenarios such as rogue USB attacks or business email compromise, or the loss of any laptop. And note how we covered how to create quality incident response plans way back in episode number 33. Go look that one up. If you want more detail on best practice on how to build cyber incident response plans.

Number three is data backups. Every company is pretty much at the risk of ransomware today, so the best thing you can do is have quality backups that allow you to recover your business operations. When your data becomes encrypted or deleted, and ensure your backups are made at a periodicity where you do not suffer business loss, if you're forced [00:08:00] to recover.

Number four restrict administrative privileges because if you reduce admin access to systems to the minimum required by a job role, this reduces the harm that one user account could cause when it's compromised by bad actors. And number five, only allow authorized applications. You might spend the time to create a Windows policy that allows users to only run approved applications.

And this means that most malware won't be on the approved list and should all be not on the approved list. It'll be blocked up front. Now notice there's workarounds in there where you could go ahead and have people come up with PowerShell scripts and the like, but in general, that helps a lot. Now there's pros and cons of each of these options, and if you don't do risk assessments, see, you might not be focusing on the right thing that needs fixing.

What if all your data is stored by a third party Software as a Service (SaaS) vendor, they may already have backups, so you might not need to spend a lot of time on that option. Instead, you might be better off implementing Windows Group policies to lock down the Microsoft Office and keep [00:09:00] macros from harming your company if bad actors can go ahead and get those to run.

And that being said, bad actors can get access to your data. Having a backup when you need to recover data is more helpful than having a risk assessment document. So talk to the executives within the company and work together to identify the appropriate level of cyber activities that the organization needs to adopt.

Now, let me share with you a post that I've found from Microsoft. It's called The 10 Immutable Laws of Security. I think you'll find this enlightening. Now, I'm not going to read the whole thing verbatim, but let me give you the rules in just a sentence or two about it, and we'll provide the link in the show notes.

https://learn.microsoft.com/en-us/security/zero-trust/ten-laws-of-security

Number one, security success is ruining the attacker's return on investment. The whole idea is, is that if you become a hard target, Even though your security's not perfect, you could make it so that the attackers are just going to say it's not worth their time going after you. They're going to move on to the next one and certain extent you win.

Number two, not keeping up is falling behind because attackers keep evolving their attacks to [00:10:00] evade your defenses. And if you build defense, they'll build a ladder. And if you build a wall, they'll dig a tunnel. So make sure you evolve with the modern safeguards and remain a hard target.

Number three, productivity always wins because if security isn't easy, then employees will work hard to bypass it. I found employees will try five times as hard to get around something they don't like. Then they just live with it. So make sure the default path is a secure path and make sure your people understand that that's a good idea.

Also, number four, attackers, they don't care if something is out of scope for your project charter or it's a legacy system that's hard for you to update, or the app that's built by your third party, which you can't patch, or is too critical to patch on a monthly basis, or it's due to retire, or just a proof of concept.

See, attackers care about their priorities and objectives, not yours. So remember that. That's not a good defense.

Number five, [00:11:00] ruthless prioritization is a survival skill. You'll never have enough resources to fix absolutely everything. Nobody does. Prioritize what you can do best. Use threat intelligence to make informed decisions and solve the issues at hand with the current level of resources that you have.

Number six, cybersecurity is a team sport. Sometimes you do things internally, sometimes you outsource, and sometimes you just buy a tool, but figure out who's best at it and adapt accordingly, because no one tool can do everything.

Number seven, your network isn't as trustworthy as you think it is. The idea of building a giant moat in a wall and doing that fortress mentality to protect our crown jewels and their citizens, it's gone. We need to make our citizens armored knights who can secure both the inside and the outside of the kingdom. Make sure you internalize the idea that your internal network could be a hostile place. It's kind of what we talk about. Zero trust, right? Treat it like one. Only authenticate users and then keep authenticating access to all the internal assets and [00:12:00] make sure that you continue to do so so that you know that you're not going to get compromised.

Number eight, isolated networks aren't automatically secure because air gap networks have been breached, but USB drives insider threats. There's other gap jumping techniques. Think about ways that bad actors might around your defenses and then plan aaccording

Number nine, encryption alone isn't a data protection solution. It's only secure as the decryption key and the algorithm, of course thats used and there's other authorized means of access. But don't assume your encryption can't be broken because we found things that get broken all the time.

And lastly, number 10, technology doesn't solve people and process problems. Humans are like the famous Jurassic part, quote by Jeff Goldblum. Life will not be contained. Life finds a way. So please consider culture training and process controls. When you think about solutions. Remember the best technical solution that's never used isn't that great of a technical solution. [00:13:00] Okay, well now that I've kept Brent waiting patiently all this time, thank you very much for doing so and listening to my monologue.

It's not as good as Johnny Carson. Hopefully helpful. We'd like to bring you on board the show and discuss now some back and forth on your approach to

cybersecurity, which also has helped you reduce the cost of your cyber insurance. So again, Brent, welcome to the show.

[00:13:19] **Brent Deterding:** Hey, thanks.

[00:13:20] **G Mark Hardy:** So tell me a little bit about yourself and your background and, and what do you do before you got here and things like that.

[00:13:25] **Brent Deterding:** Yeah, I am an executive CISO for Afni, we're about a 10,000 employee, uh, BPO business process outsourcer. Uh, I report to the CEO. I have an outstanding team of about 22 people. And, uh, prior to becoming the CISO, I worked for SecureWorks for 19 years. I was employee number 21. Spent about 15 years in operations and about four in like a salesy kind of role.

So now that many of us who came from the vendor side to be a CISO, uh, let alone from the sales side to be a CISO. Like I, I think I'm the only one, but that's [00:14:00] all right.

[00:14:00] **G Mark Hardy:** Well, that's kind of interesting. So sales, technical vendor, and the CISO role, and you've done quite well where you're at, I mean, 10,000 person organization is no slouch to be able to hold down that.

[00:14:11] **Brent Deterding:** Yeah, it's a challenging environment. I'll, I'll say that. I mean, we have all the, all the same things that any organization that size would have. It's not a hundred thousand, but, or 50,000, but it's also not 1000 either. Uh, there, there's all the challenges that come with that size of work.

[00:14:26] **G Mark Hardy:** Got it. So are there any tips you can offer pretty much for CISOs of any sized organization?

[00:14:32] **Brent Deterding:** Yeah, one of the big things to me is I, I call it, uh, accept it in your soul or internalize it, uh, for lack of a better word, that significant risk reduction is simple, easy, and cheap. So you kind of covered, what I call the hills that I'm willing to die on as a CISO, which is a 100% MFA, you are who you say you are. Device posture management. Your machine is my machine. I own that, EDR, and external patching. Uh, if [00:15:00] you do those four things, you'll be in a very enviable position, security wise, and those things are simple, easy, and cheap.

[00:15:08] **G Mark Hardy:** And so I've got the Brent Top four, and so that'll be kind of my, my new policy, so Great. And if we want to implement those, let's

say an organization doesn't have all those going, is there anyone that you would prioritize and if so, what are kind of the techniques that you've found that will convince either a user base or management of both of the importance of being able to do things such as this.

[00:15:29] **Brent Deterding:** Yeah. You know, so, yeah, I wanted to break down the simple, easy, cheap thing, right? Because simple is a technology statement. We have the technology to do MFA patching, EDR, device flash management, all this stuff you, we have, right? This is not, this is a very simple thing, right? Uh, I use Microsoft, right, Microsoft AD for MFA, I have YubiKeys rolling out a device posture. I use a second one for EDR. Like, these are things that are pretty easy to do, technology-wise, pretty simple [00:16:00] to do, but humans tend to make simple things hard, right? and there's a variety of reasons for that, but that is not a absolute requirement.

We do not have to take simple things to make them hard. So I kind of looked at it this way, with YubiKeys specifically, right? I said, okay, so if a hundred thousand employee organization can roll out YubiKeys to their entire user base and under a year, so can I, right? So it is possible. Organizations do this all of the time.

Being on the vendor side, I saw hundreds, if not thousands of more organizations who had done really cool things and they had, they'd gotten it done. So when I came to my org, I was like, well, I know this is possible, and I know that technology exists and the technology is pretty simple. So that's on me. And finally, these things are relatively cheap, right?

We have [00:17:00] MFA and all this stuff built into a lot of our Microsoft licensing that most people have. So it works, right? And as for what order implement or how to implement or any of that, I have a, an old saying that I've been using for about 20 years that is, deceptively simple and that is to, uh, get stuff done.

The same are simple, easy, and cheap. And you can, you can get it done

[00:17:26] **G Mark Hardy:** And get er done was already taken. It was trademarked, right?

[00:17:28] **Brent Deterding:** yeah, look, I don't want to be flippant about it. Um, but I do want to be, I do want emphasize that organizations of every size, vertical and complexity have done these things and done them well. They're very, very doable in almost every organization.

Hey, if they can do it, so can I. Right.

[00:17:50] **G Mark Hardy:** That's a good point because I think what we look at sometimes is we see some task ahead of us. It looks monumental and it's large, it's complex, it's difficult, maybe expensive. And we go, man, I don't know how we can do [00:18:00] this stuff. And the answer is, yes, you can. And the reason you can is it's been done before.

It's been done in many other organizations and it's been done successfully in other organizations. So I think one of the things to keep in mind is that as CISOs, we can turn to our peers. I used to say, and I probably mentioned this a couple times on episodes before, if you put the Chief Marketing officer of Pepsi and Coke in the room, they'll be in a fist fight.

But if you put the CISO for each of them, they're going to be sitting down sharing threat intel because

[00:18:27] **Brent Deterding:** security is not a trade secret.

[00:18:29] **G Mark Hardy:** it isn't, and, and nor is it really about necessarily, If at all, beating the competition because your competition is not your peer in the marketplace. Your competition is all the adversaries who would just as soon take you out as well as all the guy next to you.

And it's a matter of being faster than the person next to you, rather than outrunning the bear.

[00:18:49] **Brent Deterding:** Exactly a 100%.

[00:18:51] **G Mark Hardy:** Now have you seen the mistakes that CISOs tend to make? And if so, what advice that you might have for, for those mistakes you see in the past

[00:18:59] **Brent Deterding:** [00:19:00] Yeah, that's a, that's a bit of a bold question for me to answer. Um, but as an industry, I think that we buy an awful lot of $10 solutions to $5 problems and specifically I think that a lot of $50 problems can be reduced to $5 problems, uh, simply, easily and cheaply, right back to my old simply easy, cheap thing.

So, I'll give you, give you one example. If I have Yubikeys rolled out to my entire employee base, how much do I care about phishing? Some Do I care? Is it the biggest deal ever? No. Do I need to spend a lot of money on external

phishing tools, testing, whatever? No. Do I need, I is, is that my only line of defense against, bad threat actors?

No. Right. So like these, these things, when we, when we do these simple, easy, cheap things, they take the $50 problems and they make them into $5 problems. [00:20:00] And then I don't have to buy the $10 solution for that problem. And at the end of the day, that's decreased cost, decreased complexity, increase security.

I like it.

[00:20:09] **G Mark Hardy:** Well, that sounds like a good recipe. Now here, here's the thought. I mean, you, you mentioned YubiKeys. I think we all understand it's really useful to have some, uh, cryptographic authentication token that, you know, no, no token, no access, and I love that. But one of the things I've done in my organization, Is to implement the number matching that Microsoft offers when they'll bring up the geographic, because it's a little bit tougher to phish when you see, you know, please confirm instead of just approver deny, it's like enter the two digit number that you see on your PC screen and enter it here.

Oh, by the way, there's a map and if you see a map of East Moldova instead of a map of, New Jersey or something like that, you know, like, Hey, wait a minute, what's going on?

[00:20:45] **Brent Deterding:** Yep.

[00:20:46] **G Mark Hardy:** and,

[00:20:46] **Brent Deterding:** exactly the same, same thing that, so my org, big chunk of my org has YubiKeys. The rest are in shipping stuff. But before we did that, we, we got rid of all SMS based and all phone [00:21:00] call based, uh, authentication. Used Microsoft Authenticator and then enabled number matching, right? That was one of the very first things I did right when I came on board.

So, hundred percent agree.

[00:21:11] **G Mark Hardy:** And that's one of those things where you get the 80 20, the Pareto principle that says you get about 80% of the benefit from perhaps 20% of the activities. But the real key as a CISO, is to know what are those 20% activities that give you the highest yield? And as you'd said earlier in the show,

what hill do I want to fight and maybe die on to go ahead and push for it because, As a vendor and I've, I've worked in the vendor world before myself.

Your solution always looks great, but reality is, is that it may not be what you need and you want to be careful as a CISO that you are buying solutions not being sold solutions.

[00:21:44] **Brent Deterding:** Yes.

[00:21:45] **G Mark Hardy:** So what advice would you offer for someone to, to make sure, particularly with RSA coming up and you go there and just the amazingly huge spread of vendors and you get the bags to fill up with tchotchkes and things such as that.

And you end up on these email lists because they [00:22:00] scan your badge and off you go. But where's someone to be going to one of the major shows in the near future, any strategies you might have for how to better prepare for those.

[00:22:11] **Brent Deterding:** So one thing that I really do that, that I like my number one question and I ask this question of myself. I ask it to my team, I ask it to vendors. I ask it all the time, and that one question is, tell me a plausible story where not having your solution or not doing this thing costs my organization money, right?

Because at the end of the day, my job as CISO is to mitigate material risk, right? Prevent the organization from doing the really, really bad risk so that we can take and make good decisions about the good risk. It is not to eliminate risk. And so in order to eliminate the material impact events, the the big, big deals, right?

Then I need to be able to answer the question and articulate that answer, well, [00:23:00] why did I spend this minute? Why did I spend this dollar on this solution? How is it enabling the business? Right? I enable my business in four ways. That is compliance, cost avoidance, increase the efficiency in enabling sales, right? So everything I do ties back to one of those, which is another way of saying, tell me a plausible story where not having this cost my organization money if I did nothing. What would that, what, what's the downside? Is, is the world going to blow up? Am I going to get ransom in a heartbeat if I don't have this? Maybe, and that's why I do those things. Or maybe it's like, eh, I can't really justify the the spend here, right? It's the $10 solution, $5 problem thing,

right? So as you go through RSA or whomever, or as you talk to a vendor, or as you look at yourself or as you talk to your team.

Ask your yourself, how is this enabling my business? If I don't have this, how's it costing me money? Is that story [00:24:00] a plausible story? All of these are different ways of answering, of asking and answering the same thing, and I think that it is critical to answer. Now, uh, I will give you fair warning, bill, if you start doing that. For one thing that you're doing, then you're going to have to do that for everything else that you're spending money and time on. And you may find that you don't need to do some things that you're currently doing and you may also find like, upon him saying that I may not like paying taxes, but I have to do it anyway.

I may not like some specific part of PCI, but it doesn't matter. I've got to be PCI compliant to be in business. So some things are just, the risk of addressing is compliance. We must be compliant. We must do this. Like it not, doesn't matter, do it. So, always ask, always ask, how is this enabling the business?

[00:24:53] **G Mark Hardy:** And so I took notes on that one. And the four things that I got, correct me if I'm wrong, compliance, cost effectiveness, [00:25:00] increase your sales, and increase your efficiency. The ladder, two being basically business functions and the first two being, if you will, the IT or the cyber functions.

[00:25:09] **Brent Deterding:** Yep. Pretty much.

[00:25:10] **G Mark Hardy:** yeah, and in a way we're in the business of revenue protection, but also business enhancement.

We, for anybody who wants to think of cybersecurity as the cost center, then you can remind them that we enable the organization to do business and collect revenue and make profits in ways we could not do unless we were secure. And, you know, pci, you mentioned that what if the majority of your sales come in through credit card sales, which most organizations do unless they do purchase orders, and we have to be PCI compliant.

Failure to be PCI compliant means that, well, they may or may not yank your credit cards, but if nothing else, you have to. Outsource to somebody else for every single charge, and that's potentially lost revenue. At the same time, from a risk perspective, I can go to an authorized Dot net and said, Hey, you own the risk.

I just don't want to touch anything that has to do with credit cards. Uh, then your PCI compliance audit goes very, very quickly because you're like, Hmm, no, no, no. Don't do that. Don't do that. Things [00:26:00] like that.

[00:26:00] **Brent Deterding:** You know, my friend, Malcolm Harkins, former CISO of Intel, I love his analogy. The best of the CISO's job is, excuse me, kind of like the wing on a Formula One race car, right? That wing creates friction. But it creates friction to enable the car to go faster. Right. And I really like that analogy. Like there is some level of friction, right?

That CISOs impart to the organization, but that is a very good thing because it doesn't slow you down, it enables you to go faster. Right. Done. Well that's, that's the goal anyway.

[00:26:36] **G Mark Hardy:** Yeah, it lets you go fast. Although the same thing. You know the question. I remember that Jeff Moss had mentioned this when I talking to him. He said, why do race cars have really big breaks

[00:26:46] **Brent Deterding:** Yeah.

[00:26:47] **G Mark Hardy:** So they can go faster? Right. It's not so they can stop because. If you think about it now, we don't want to be viewed as a big break on the organization, but at the same time, yeah, we can go ahead and if we have to, you throw [00:27:00] the red flag and say, no, this is a real high risk.

And from time to time you need to go ahead and uh, and pull out that trigger and say, this is an issue.

[00:27:09] **Brent Deterding:** You know, I loved it. I was like three weeks into being a CISO and one of the HR directors called me and said, Hey, I hear you are the yes how guy? I have a problem. Can you help me solve it? And I was like, Touchdown victory. Like that's awesome. As the CISO to be like three weeks in and someone's like, I hear you're the yes how guy?

And I'm like, yeah, let's go. Let's figure it out. Right. And we did. We found out a solution that solved her pain point and what ended up like in a secure fashion. And it was great. Right. So there's a lot of like increased efficiency. There's a lot, there's a little bit of friction. There's, it's, it's all the same, but everything goes into enabled the business, right?

Every single thing is enable the business.

[00:27:55] **G Mark Hardy:** Now, and that makes really good sense and and I absolutely agree with you. So if we're focusing on enabling [00:28:00] the business, but yet we recognize we're either going to be a wing or large breaks or something, we're going to have to apply friction where necessary. I think it makes sense if we're going to do that, to do it in a strategic manner. And one of the ways we do that is with existing frameworks, for example, ISO 27001 or the NIST Cybersecurity Framework of things such as that. So in a situation like that where maybe you had not been using that type of a framework, but you go, wow, we really should. Any thoughts about, Hey, which one do you pick?

And then how do you get it going? And then ultimately get to the point where that is how you're, you're measuring your cybersecurity effectiveness.

[00:28:36] **Brent Deterding:** Sure. So I differ from almost all of my fellows or colleagues. Um, I don't really care for frameworks. I don't, I don't adhere to one. I don't have one or, well, uh, let me clarify that. I have one, but I don't know anything about it. I think that frameworks can be immensely useful to increase the efficiency of some processes [00:29:00] from a risk reduction perspective.

I don't find them to be valuable. Now, this is, uh, many people disagree with me on this. Um, My perspective is that I mitigate material risks. That's victory. That's my job as a CISO. So that's what I do. I don't need a framework to identify and mitigate material risk. I don't need a framework to prove my worth to my executive team.

Um, my value is evident, all involved, and if it is not evident, then I should probably step down and go do something else where, where my value is evident. That's a bit of a controversial opinion, but that's, uh, that's where I stand on it. I don't find frameworks to be incredibly useful. A lot of people really, really like them, specifically to measure maturity scores and things like that.

Um, I don't, and my executive team agrees with that. My exec team has no use for them either, so,

[00:29:53] **G Mark Hardy:** What's interesting, Brian, because in some organizations though, you're, you're rather constrained to that. If you're government, government contractor, things such as that. You [00:30:00] walk in, the inspectors walk in the door and you say, why are you here? We don't do Yeah. Like frameworks. We don't need no stinking frameworks.

[00:30:07] **Brent Deterding:** That's, that's where I am.

[00:30:09] **G Mark Hardy:** And that's where you're, and uh, but therefore if we have an approach, let's, let's go back because we talked a little bit earlier, I think before the show about standardizing on a vendor and, you know, we'd done an episode 114 on talking about how you could adopt the Australian eight. The Essential eight and pretty much with Microsoft.

So, uh, Microsoft, in my opinion, has been doing more and more to fill in the gaps in their coverage over the last several years. Good on them. A little bit scary if you're a vendor who fills a gap that existed in the past and the Microsoft says, oh yeah, we fully cover that and it's organic and worse yet if it's included, it's part of the price.

And I don't think you're going to be able to go ahead like Netscape did and argue with a antitrust suit that the, the embedded Internet Explorer browser, Uncompetitive and you got to peel it out. So what do you think is a benefit [00:31:00] for CISOs pushing for primarily a single vendor solution?

[00:31:06] **Brent Deterding:** So count me on team platform. Uh, you know, the, the standard line is the, uh, best of breed point solutions or good enough for the platform. Um, I don't happen to buy that, but let's say I did even for a minute. I don't need best of breed to suit my needs. In most cases, I'm doing a bunch of things, mostly because some compliance says things, says I have to, and doing that as part of an integrated platform suits me just fine.

Right. Um, I. You know, I, I, uh, I also scratch my head a little bit when I hear the standard statements from Forrester and whomever else they say, you know, the standard, the enterprise has 70, a hundred, 140 different tools for security. And I'm like, huh? Like, I have like 10. And I argue that that might be more than we need, right?

[00:32:00] Maybe I'm counting things differently that I, I don't know. But I like the platform approach because even if a different solution is a little bit better here or there, that's probably functionality I don't need because of my simple ec cheap approach, right? Because of, you know, MFA and YubiKeys and device posture and, and all that conditional access, right?

Such. My users are who they say they are. They're on my corporate machine. It has EDR and everything externally is patched. If I have that environment, I don't necessarily have to worry about higher end little minute differences here and there and and point solutions. I'm want to go for the integrated simple approach, right?

Mash that easy button is my kind of internal catchphrase. This hit that easy button.

[00:32:50] **G Mark Hardy:** Now sometimes CIOs get a little bit worried about vendor lock-in and is that something CISOs ought to worry about, that they're putting too many eggs in one vendor basket or what do you think?

[00:32:59] **Brent Deterding:** [00:33:00] You know, uh, I'm going to say something that you're, you're, I'm going to say it and you're going to have to give me a second to clarify it. Cool. So, I was, I was the cloud guy, uh, and back in like 2016 when no one like knew anything about cloud and this is where the Office 365, uh, Amazon data, this is where all that really kind of started.

A lot of the eggs in one basket, fox watching the hen house, you know, all, all that stuff. And most of the people that I heard say that in 2016 are now retired. I've not heard that many people say that who are under the age of 60. Now I am not saying like there's two possibilities there, right? One is that a lot of those people who said that, um, are very wise and have learned a lot of things that that us young whipper stampers don't appreciate. And the other is that they're not [00:34:00] willing to do things differently or change or, or whatever else. I'm not saying which one is right or wrong, but I am saying that I don't have that fear, especially when I look at the massive investment of billions of dollars Microsoft just made for years and the amount that they're going to be making.

And the same is true of Amazon and Google and all these people, like people respond to their incentives and Microsoft, Google, Amazon, all these people, their incentives are for security, right? So I can go with that. I, I like that. I don't have any issue with all my data being Microsoft. I don't have issue with Microsoft Security Stack.

I don't have an issue with that. not at all. And I increasingly, I see that as a, Less common opinion that people have. I think, I think we've really kind of moved past that as an industry.

[00:34:53] **G Mark Hardy:** So you're basically saying, uh, by Microsoft and short, all the small vendors

[00:34:58] **Brent Deterding:** Well, but you know, a [00:35:00] lot of those small vendors can work with Microsoft or against Microsoft,

[00:35:03] **G Mark Hardy:** or, or they get bought out by Microsoft. They say, we like that gulp, and you go,

[00:35:08] **Brent Deterding:** yeah. And you know, like, hey, everything that Microsoft does, I don't buy every, every single thing. It is quick. I, I can tell you that when I'm renewing my vulnerability management in a year, I can tell you that they're going to be part of the conversation, right?

Microsoft is, is going to be a, a competitor in, you know, my MDR and my PAM and my vulnerability management and they're already in for MFA and my SIEM and all this other stuff. Like they're going to be in the conversation they have earned a seat at that table

[00:35:40] **G Mark Hardy:** and I'm having some interesting conversations with one of my senior IT staff members who's saying, we don't need these other tools. You don't need your mdr, , or, or your managed, , services. We don't need to have, let's say, this particular EDRs tool will just go ahead and use defender, et cetera, and, and my approach as a CISO is, well, I don't want [00:36:00] to fit the pieces the armor so that there's just a single seam and there's no overlap. I like overlap and more comfortable. I don't mind spending a few hundred dollars here. There are a few thousand, not a ton, but enough to say I've got a second line of defense in case somehow someone cracks. because after all, if you're the biggest vendor out there, you're going to be the biggest target out there and your time when a zero day is discovered to when it's fully patched in your environment, let's face it, that's a vulnerability window and we have no control over those. Um, so thoughts on, uh, you know, the Belt and Suspenders approach.

[00:36:35] **Brent Deterding:** Yeah. I think that in many cases, like I go back and say, tell me a story where this costs me money. Right? So, okay, uh, do I care, do a thought experiment with me, right? If all of my internal systems, if I don't have any patching whatsoever, but I have mfa, YubiKeys, device Management, EDR, [00:37:00] do I care? Maybe, I don't know what your org is, right?

Are you worried about a malicious insider who's going to pop a a zero day against a vulnerability? Are you worried about someone physically getting on your network and doing that? Are you worried about a nation state level attacker? If you are, Hey. All right, cool. Uh, but for most of us, like now, should I, should you still pass?

Yeah, because it's not hard. You can automate most of it and it's relatively easy, so Okay, fine. All right. If you go into those decisions with your eyes wide open and say, I am accepting this risk of this odd thing happening in order to save this

money and decrease complexity by here, by going with the vendor, then that's fine.

You are able to make that decision. You and your organization are able to make that. Um, what I've seen more often of is more often I see the knee jerk reaction. I'm saying, we must do, you know, two is two is one, one is none. That, that kind of [00:38:00] thing. And I, I think that it's more nuanced than that. That's a really good way to spend a whole lot of money fast, right?

[00:38:06] **G Mark Hardy:** Yep. So let, let's, let's look at one other way to spend money because we're getting down to the last few minutes of the show. And that's cyber insurance. Now as we've seen, rates have gone up, the questionnaires have gotten longer, uh, it's sometimes it's, it's getting to be the pain where all of a sudden it's like, wow, we're not, or this is kind of looking forward to it, like you're, Your, proctology exam or something like that.

It does not look fun. Uh, but anything that you've found that's helped out for CISOs with cyber insurance, what helps them get the best deal? What helps them keep the objections down? And, uh, any words of insight or wisdom that you've got there?

[00:38:42] **Brent Deterding:** Yeah. Uh, webinars and articles and blog posts abound on this topic, right? And I think I, I think I've read and attended all of them. So I spent my first year as a CISO implementing my Four Hills strategy, right? And giving my integrity team updated on the market. Every, every [00:39:00] webinar I did, everything I read over your Wall Street Journal article I sent said to expect a 20% increase in premiums.

Now, our premiums, we kind of got lucky. They were a little bit low for reasons unknown to me. Uh, so my broker said, eh, you might go up more than 20%. So the broker had told, my CFO had told me, Hey, expect your premiums to go up probably more than the market, right? And the market is 20%. Okay. I presented my program and my four hill strategy to with two slides and about 10 minutes to about 15 different underwriters.

My first slide was those four hills, right? Mfa, EDR, device, posture, external patching, and the second slide was a huge list of all the things, right? That whatever, yes, I have policies, yes, we have backups, yes we do whatever. It's all that table stake stuff, right? So, And then I answered a couple very, very specific questions that they had.

[00:40:00] And, uh, my premiums went down by a third So my premiums are anecdotally 40% of what I hear other CISO saying for the same coverage. I've only done the cyber insurance thing once, but it would appear that I'm doing okay at it. So

[00:40:17] **G Mark Hardy:** do that with property insurance in Florida, you'd be really, really popular. I went up 150%. I ended up jumping ship to another company. It's like nothing has changed. I, there's nothing more I could do. I mean, yeah. But, uh, sometimes they decide, Hey, we need more money. Uh, or we made bad risk decisions in the past as an insurance company.

And we need to do that. So your four hills will I, I like that because it's a good way to summarize that. You've got, if not, it's a formal external framework. It is your framework and it works and it really represents best practice. And then to be able to go through and say, but we implement it, not just conceptually, but here, here, here, here, and here.

And, uh,

[00:40:57] **Brent Deterding:** I took the approach of being empathetic [00:41:00] to, um, I, I, I put myself in the shoes of the underwriters and I said, if I'm an underwriter and I'm evaluating this guy and his company, like how likely is this guy going to cost my company money? Like, how, how likely am I to pay out a claim? And so I took that and I said, man, if I was an underwriter, I would want to hear that they have identity locked up like mfa.

And if they say YubiKey is like, I know where YubiKey is, that's awesome. And EDR is a big deal. And then I said, device posture. I'm like, what's that? And he explained to me that, oh, that means only our corporate systems can connect to anything about our environment. And they do external patching. We're like, dang, I want to take that guy's money.

I will sign up every day to take that guy's premium and that worked. So I never a reference maturity score or a framework or compliance, anything. I talked about my four hills and that I list literally big list of all the other things that we do [00:42:00] and

[00:42:00] **G Mark Hardy:** Yeah, and I love, and I love that, and I think we might borrow that and, uh, as, as a recommendation, at least, I might try to anyway, because I'm doing those things. We haven't articulated them, I think as cleanly as you have, but your point is extremely, well taken. We often think of a role as, as CISOs, as reducing the risk for our organizations, but the reality is

you put yourself on the other side of the table when you're negotiating with someone like an underwriter to say, I'm going to reduce your risk as well.

In fact, my goal is every time I write you a check that it's money out the door, because you're never going to have to do anything other than pay the cash to check and then send me a receipt. Now, that's the perfect customer to have if you're an insurance company. But try to convince him of that. And you'd mentioned you had multiple underwriters.

Did you do that kind of like a bidding war? You get them all in the same room, you said, all right, here y'all have paddles. Or how, how? How did you do

[00:42:48] **Brent Deterding:** Al, almost. So what was crazy is that you hear all the, these incredibly long, uh, questionnaires. I filled out one fairly short questionnaire from my broker. My broker had all [00:43:00] the underwriters on the phone. I don't even know what all providers were on the phone, and I don't know what happened on the backhand.

All I know is that like two weeks later it came and it's like, Hey, your premiums are a third less. And I was like, Hey, that's a victory for me, right? My CFO love that. So,

[00:43:14] **G Mark Hardy:** Yeah, that broker, you need to go ahead and, uh, buy them an ice bottle or something or other if they, if they're so inclined, could they definitely save you some money? because that's, that's a great thing to do. Hey, any last thoughts before we wrap up here? you've given us a whole lot of insights and wisdom, some great ideas and things such as that.

I've, I've tried to take some notes, although I don't think I've done it justice on the fly. So the nice thing is we'll have transcripts and things like that as part of the show, but how would you like to wrap up?

[00:43:36] **Brent Deterding:** Yeah. You know, I, I think it's, very powerful to, internalize the idea that significant risk reduction is simple, easy, and cheap. And that seems to be counter-cultural a little bit, but I really do believe that it is, and I think that I've, proven it, at least in my organization. Mine is not the only out there.

Obviously, we all have different orgs, but I think that the principles apply very well. [00:44:00] And, uh, thank you very much for giving me a platform to talk about this.

[00:44:04] **G Mark Hardy:** Well, Brent, love having you on the show. I think you've added a lot of wisdom for everybody. And to our audience, thank you for tuning into another episode of CISO Tradecraft. We hope that this has been a worthwhile investment of your time. This is your host, G Mark Hardy, and we encourage you if you're, again, if you're not watching us on YouTube, please do so.

Other than just looking, look at my smiling face and Brent's smiling face. Uh, it also helps build our reach out so we can help other CISOs as well in their careers. So thank you again for your time and the investment, and until next time, stay safe out there.