In the Trenches

Episode Transcript — Cybersecurity 101 for Small Businesses

STEVE 01:29

Hello, everybody, and welcome to another episode of *In the Trenches*. I am your host, as always, Steve Divitkos. When I was running my company, I recall being vaguely terrified at the prospect of falling victim to a cyber attack. Not only did the threat seem more likely with each year that passed, but it also felt like its potential impact grew as we acquired more customers, hired new employees, and put more of our internal systems online.

Today, in 2026, you probably don't need to look terribly far to read about both the frequency and the seriousness of cyber attacks on both individuals and on small businesses. Because of how unfortunately common these attacks have become, and because of how difficult they can be to understand if not properly explained at the appropriate level of detail, I thought it would be worthwhile to dedicate an entire episode to what I will refer to as Cybersecurity 101 for small businesses.

To help me with all this, I was joined by Kip Boyle, a security expert with 25 years of experience in cybersecurity and IT risk management for organizations in insurance, financial services, technology, military, and logistics, among others. Prior to his current role as a consultant and fractional Chief Information Security Officer for small businesses, Kip spent many years as the Chief Information Security Officer at PEMCO Insurance, and has also served as the Chief Security Officer of a transaction processing business and an IT services provider to financial institutions.

In our discussion today, among many other topics, we will cover the most common cyber vulnerabilities for small businesses, the minimum viable cybersecurity stack for small businesses, how to build out these types of internal capabilities if you don't have IT leadership or even an IT employee, when outsourcing to a separate company is a good idea and when it isn't, whether the growth of AI tools is a net positive or a net negative for small business cybersecurity, the role that cyber insurance should play in an overall protection plan, and much, much more.

But before we dive into any of that, allow me to conclude with my usual reminder that I am an active investor in search funds and the companies that they acquire through my firm, Mineola Search Partners, which is now investing out of its recently launched second fund.

So if you're looking to raise a search fund yourself, or if you have an equity gap, I'd welcome the opportunity to speak with you. But for now, I hope you enjoy today's conversation with Kip Boyle.

STEVE 04:05
Kip, welcome to the show.

KIP BOYLE 04:07
Hey, thanks for having me, Steve. I'm really excited to share some information that I hope your audience will benefit from.

STEVE 04:15
Great. Well, we're excited to hear it. And maybe before we get there, let's set the table a little bit. Tell us about yourself, your career, and what you're doing today.

KIP BOYLE 04:26
Yeah, happy to do it. So I've been working in what we call cybersecurity now for a while. It started when I was in the Air Force way back in 1992. I was a captain in the Air Force. I worked on some top-secret weapons development programs, and that's how I learned to do data security and system security — it was required in order for me to go to work every day, to open the big door to the vault and step in. More recently, after I left the Air Force, I was the Chief Information Security Officer at a regional property and casualty insurance company called PEMCO, based here in Seattle. And in 2015, I founded my own company called Cyber Risk Opportunities. I've also written a couple of books. One of them is called *Fire Doesn't Innovate*, which treats cyber as a business risk — I wrote it for senior decision makers who need to understand what this cyber stuff that everybody keeps talking about actually is, and more importantly, what to do about it or how to think about it.

And I have another book coming out this fall called *Gears Don't Guess*, which is designed to help the same audience answer the question: what do I do about AI? When is it okay, when is it not okay? So I guess if I have a superpower at work, it's helping non-technical leaders understand this sometimes very technical cybersecurity stuff. And I think the bottom line is: you don't need to understand it deeply, you just need to be a good manager.

STEVE 06:20
Yeah. Good. And we're going to get into all that. Before we do, I'm just curious — we're speaking to a group of entrepreneurs here. What compelled you to take the entrepreneurial

leap? You were a C-suite executive at a large insurance company. That's often not the hotbed of entrepreneurship. And you decided to hang out a shingle and do your own thing. I'd love to understand how you thought about taking the plunge, so to speak.

KIP BOYLE 06:47

Yeah. I think the most direct line I can trace for you goes back to an educational opportunity the insurance company gave me at Seattle University. They had an executive leadership program — a two-quarter certificate program — and if you wanted to go further, you could get an MBA. They sent me to the first two quarters to get that certificate. Because I grew up — professionally, I mean — in the systems world, but when you're operating as a senior decision maker, you need more than the technical expertise you've gathered. You really need to flip the way you see the world at work. So that course was a really important, formative experience for me.

One of my big takeaways from it was: impact. How can I have the greatest impact? How can I help the most people? I realized that when I was about seven years into the insurance company, I was a little burnt out. I started asking myself how I could have more impact. And I'd always kind of wanted to have my own business — just an itch I'd always wanted to scratch. So I thought, let's see if we can put those two things together. And eleven years later, it seems to be working.

STEVE 08:21

Love it. Okay. So, like we discussed before we hit record, generally the folks listening to this will be small and medium-sized business CEOs, or those looking to become one. Generally speaking, non-technical — though there will certainly be exceptions. Where I want to start is with a batch of questions I might loosely describe as Cybersecurity 101. Let's start with the basics, the must-haves, the fundamentals. Given your experience working with a large number of businesses, if you look at a typical small or mid-sized business, are there a handful of common cybersecurity vulnerabilities that you encounter? And are there any that tend to be particularly acute in terms of the risks they present?

KIP BOYLE 09:09

Absolutely. First thing I should preface my answer by saying is: cyber is a dynamic risk. It's not a static risk. And this is one of the big takeaways from my book, *Fire Doesn't Innovate*. It's really important for senior decision makers to understand this because just when you think you've got it all dialed in, some cyber criminal will find a new way to mess with you — and you won't have it dialed in anymore. So you need to expect and be okay with an

ever-rising bar for how you need to protect your organization, your digital assets — which would include your money, your reputation, and so forth. I just wanted to make sure that big-picture piece is out there before I start talking about specifics.

And actually, we're in a good position today, because when I first started working in cybersecurity, nobody really knew what worked. It was just sort of like folk art — we were just trying to figure it out. What we have these days is data. So the answer I give you today is going to be based on rigorous data. Marsh — part of Marsh McLennan — is an insurance broker and they've studied thousands of companies. They actually modeled cyber risk the same way an insurance company might model hurricanes: super sophisticated. And so let me tell you some of the big gaps they've identified.

The first one is identity. In other words: how do you know that the people accessing your digital assets are the people who should be accessing them? This goes back to phishing, stolen accounts, stolen passwords. Most of the problems we deal with today are around bad assumptions about who's in our systems, and so a lot of it has to do with identity. Everybody's heard about multi-factor authentication — well, that's really where it's at. And I would say that's the number one thing, because a lot of organizations of the size we're talking about are very hesitant to turn on multi-factor authentication. They think it's going to turn them into a bank and they won't be able to get anything done — they'll be all process-bound, just authenticating all day long without ever getting any work done. And trust me, I've talked to plenty of people in this situation, and I'm giving you the polite version of what I often hear.

STEVE 11:56

That's so surprising, because as someone who uses multi-factor authentication myself, I appreciate that it takes, you know, a couple of seconds.

KIP BOYLE 12:04

Well, that's because you've taken the time to do it. But for people who don't do it, it really just sort of has this connotation of — well, when you go to the airport to get on an airplane, you know you're going to have to go through that gauntlet called security. And you can pretty much bet it's going to be a long wait, it's going to be boring as hell, you're going to get hot and sweaty, people are going to do things that irritate you. And that's what a lot of people think about when they think about multi-factor authentication. It's like: I don't want to have to fight through the security screening process every time I just want to use my computer.

STEVE 12:45

Yeah, interesting. Okay. So identity is number one.

KIP BOYLE 12:48

Yeah. I think that's number one, and I'm going on the data. The next thing is an incident response plan that you've never tested. The reason why this is important is because I see people do this all the time — they either don't have a plan at all, or if they have one, it's just sort of one you can wave at an auditor or at the insurance company if they ask whether you've got one. But it's not really a working document. It's not really an SOP. And the thing about it is: when something bad happens — and it's going to, everyone's going to have something bad happen to them, it's just the nature of the internet these days — the last thing you want is an adrenaline-fueled response with no guardrails. That's where a lot of people actually make the situation, which is already pretty bad, even worse, because they're just flailing around. They've never dealt with this before, they've never even thought about it, and all of a sudden they have to.

If your listeners would like a real-world example of this, there's a case that was written up based on an interview with the CEO of a business called United Structures of America — because that company got hacked out of business. They went bankrupt. It was a mid-sized company, about 200 employees, that made steel buildings. And this CEO was just fearless the way he debriefed what happened to them to a Wall Street Journal reporter. I can't recommend it enough, and I'd be happy to give you the URL. It's very easy to see yourself when you read this interview, in terms of what you need to do.

STEVE 14:42

Interesting. Okay. So identity is number one, lack of a response plan is number two. What are some of the other big ones that stand out?

KIP BOYLE 14:52

Another big one is: everybody is the administrator of their own computer. That kind of makes sense because then they can fix whatever's wrong themselves if something doesn't go right. Small companies don't tend to have a big IT department — or maybe they don't have any dedicated IT person at all for a long time. So you'd think, yeah, people are just going to self-help their way through IT problems. But the problem with that is: if the people attacking us can get hold of our account by stealing our identity, well, then they can do whatever they want. It's a very thin door between an outsider and an insider.

So the right thing to do is to have people log on using a non-administrative account. You can give them credentials that will let them become an administrator for a period of time if they need to troubleshoot or change something — they just don't want to be processing email or surfing the web while running as an administrator of their computer. That's a big difference. And this is one of the low-hanging pieces of fruit — just make that one change and it's going to cause the number of incidents you can expect to experience to go down, without drastically driving up your overhead.

STEVE 16:18

Got it. Okay. I do have a follow-up, but I want to make sure we go through your entire list of common vulnerabilities first. Is there anything else to add?

KIP BOYLE 16:27

Well, the thing about it, Steve, is that the list is almost endless. I don't want to overwhelm people. Let's just stick with these few things because I think they're the top ones. And if somebody's listening and thinking, I don't know where to begin — pick one. Pick one of the few I just gave you and just start working on it and go from there.

STEVE 16:49

Okay, so let's focus on the three you've mentioned: identity — which includes phishing, multi-factor authentication, stolen passwords, et cetera — the plan or policy or response document, and then the everyone-is-their-own-administrator dynamic. In light of the fact that these tend to be rather common points of vulnerability, if I were to ask you to build — and it's an unfair question, of course, because every business is different — a minimum viable cybersecurity stack for a typical small business, what would you put in that stack that you think is mandatory? And are there any tools that are commonly recommended as being mandatory that maybe you think are actually closer to optional?

KIP BOYLE 17:36

Yeah, well there's a lot of optionality, and it's going to depend a lot on the size of your organization — because some things would be great to have but quite frankly require a full-time person to operate them. If you're not large enough to afford that, either as a direct hire or through an MSP, then it just doesn't make sense to even consider it. So first: multi-factor authentication is absolutely required. I wouldn't even make that optional at this point.

Now, I'm not happy to tell you that today a lot of people get their multi-factor authentication as a text message — you log in, you get a text, you copy that six-digit code over. Well, unfortunately, that's a completely compromised way to do it. It used to be secure, but cyber criminals have figured out how to hack that to death. And beginning this fall, Microsoft is actually turning that off — it will be fully turned off by February. So whether we like it or not, we're going to have to stop using text-based forms of multi-factor authentication and move to other methods that are more secure and genuinely better.

So that's one thing. The other thing is you want some kind of an endpoint detection and response package. For people who've been in the working world for a long time, you probably remember when you could just buy a subscription to Norton Antivirus or McAfee, put it on your computer, and pretty much forget about it — renew the subscription once a year. But that's not the right way to think about it anymore. You need a more advanced program that's not just going to do antivirus, but is actually going to be able to find malicious code that's never been seen before. Endpoint detection and response — EDR — is what you really want to get. And there's an easy way to do that if you're in the Microsoft 365 ecosystem: use Microsoft Defender, or Windows Defender. Depending on what license level you're at, you may already qualify to have it for free — you just need to turn it on. And it's actually very good. I know that people who've been in the working world for a long time might be skeptical of a Windows security product, but Microsoft has gotten so much better at securing their tech stack that it's actually flipped and is now the better choice.

STEVE 21:00

Okay. So we have multi-factor authentication turned on, we have this endpoint detection system provided by Microsoft — or are there other vendors you would recommend outside of Microsoft?

KIP BOYLE 21:15

Actually, I wouldn't. At this stage of our overall technology evolution, Microsoft is top three and has been top three. And the price point is very, very good. Plus, it's being published by the same company that builds Windows, so they deeply understand how to have an endpoint detection and response system that doesn't crash your machine all the time — which can be a problem with third-party packages. Are there other ones? Yes. But I wouldn't start with them. I'd only go to them if you had a very specific reason.

STEVE 22:08

Okay. Anything else you'd put in this minimum viable stack?

KIP BOYLE 22:12

Yeah. Make sure you're getting email filtering — and not just spam filtering. You want heavy-duty email filtering where the message comes in and, if there are any URLs in it, the email system actually tests each one of those URLs before delivering the message to you. It can detect malicious links and either alert you to them or quarantine them. That's a huge thing you're going to want to do.

If you're sending marketing messages as part of your sales and marketing, you're going to have to get really good at these anti-spam systems — Google now requires them in order to have good assurance of deliverability to Gmail users or anyone in the Google tech stack. And as you do that, protect yourself too, because there are some very simple things you can enable that will greatly decrease the chance that somebody can spoof or pretend to be someone in your organization by using a look-alike domain. So get really good at email filtering — both for the marketing emails you send out and for the emails you receive.

STEVE 23:54

What do those anti-spoofing tools look like?

KIP BOYLE 23:57

Well, SPF is one of the protocols, and that's an awful little acronym — let me decode that for you, because there are some other related protocols I should tell you about. SPF stands for Sender Policy Framework. A bunch of really smart engineers sat down and figured out how to make sure that when you send an email, the machine that receives it can say: "yep, this is an email from Kip," as opposed to an email from somebody claiming to be Kip. And conversely, when you receive an email, you have some way of knowing it came from Kip and not somebody who's impersonating Kip.

Now the good news is you don't have to be an expert on this. You just need to go to your email provider — whether it's Microsoft 365 or Google, whoever — and talk to them about getting anti-spam protection set up. You can mention SPF, and inside of that there are a couple of related acronyms. One is DMARC and another is DKIM. I'm only telling you this because your listeners don't have to understand what these acronyms mean — just say them to your friendly neighbourhood IT person and they'll figure it out and know exactly what you're talking about. So: SPF, DKIM, and DMARC — those are the three you want your IT person to turn on for you.

STEVE 25:55

Those who have had email deliverability issues are unfortunately likely all too familiar with those three acronyms.

KIP BOYLE 26:03

Yeah. But they're probably only thinking about it in terms of outbound — like, I want deliverability for the messages that I send. And that's why I want to make the point that if that's already something you're paying attention to, well, it's just a little extra effort and you can protect yourself on the inbound side too.

STEVE 26:21

Yeah. Okay. Keep going, if there's more to include in this minimum viable stack.

KIP BOYLE 26:27

Just a couple more things. You need good data backup. Good data backup will save you — it will absolutely save you. If you read that Wall Street Journal article I mentioned about United Structures of America going bankrupt, that's a huge theme the CEO talks about. They had spent tens of thousands of dollars on a good data backup system. It was installed, all the lights blinked, it seemed like everything was doing what it was supposed to do. But when they got hit with ransomware and said, "no problem, we'll just restore from backup," it turned out their backup system had never been configured correctly — their tapes and all their systems were empty.

STEVE 27:14

Yeah, exactly.

KIP BOYLE 27:15

So it was awful. That's because they never tested it. You need good data backup, but you also need to test it to make sure that when you need it most, it will actually help you. Okay? So let's stop there — I've just given you four things you can start with. I don't want to overwhelm people.

STEVE 29:04

So let's talk about this idea of overwhelm, because I'm fairly certain that most CEOs listening to this either don't have an IT department, or if they do, they don't have an IT leader — it's more like individual contributors configuring new users and new hires and that kind of thing.

KIP BOYLE 29:24

Yeah, maybe a part-time contractor.

STEVE 29:27

Something like that, right? And so I'm putting myself in the shoes of a small business CEO listening to this who is drowning in all sorts of other business problems, and they hear all these things you're saying that sound like they're in another language — and they feel very daunted at the prospect of implementing this stack by themselves. Maybe speak to that person. What would you say to someone who's feeling all of that right now?

KIP BOYLE 29:49

Yeah. Well, the first thing is: hey, guess what? I'm a small business owner too. We're in our twelfth year, and I have eight people who report to me and customers all over the world. So that's the first thing you need to understand — I totally get what you're saying. Even though I understand all of these acronyms and I understand the ones and zeros, I also understand what it's like to be trying to find product-market fit. How can I offer something that people will actually want to buy from me? If I can't figure that out, then none of the other risks I'm facing are really that important. None of the stuff I'm talking about makes any difference if you can't set up a reliable system for generating revenue. So if that's where you're at right now as a business owner, that's really what's most important. Don't get sidetracked on all this cyber stuff, because the last thing you want is a very, very secure system that isn't bringing any revenue. Cyber is just a risk you have to deal with, but sometimes you have risks facing you that are far more existential and those have to be sorted out first.

Now, assuming you don't have an existential risk facing you — well, now you've potentially got some bandwidth for dealing with this. And you probably should get some help. Not because you can't do it necessarily — I'm not suggesting that if you wanted to sit down and learn it, you couldn't. You probably can. However, as a small business owner, I know that a huge part of what makes my success possible is delegation. I have to get work done through other people. If I try to do everything myself, I'm going to burn out. So I've got to get really good at having other people get stuff done. And that is how I would encourage you to think about this cyber stuff — make the decisions about what you want to do, pick one from the list I've given you, find somebody you can hand it off to and say, "this is what I need," get it done that way, and then go back to dealing with the things that only you can deal with.

STEVE 32:32

So that brings to mind the question of outsourcing, and we're going to get there. But before we do, there is a temptation — an understandable one — to throw software and technology at this problem. To spend a lot of money and time on software and technology to protect against this risk. But I wonder if you can make the opposite case. Can you explain a line of thinking or a situation in which throwing money and technology at this problem is actually not the right thing to do? The reason I ask is that in my very limited understanding of all of this, I think the most common entry point into an organization is a human clicking on something they shouldn't be clicking on. And that doesn't seem like a technology problem — it seems like a human and awareness problem. So I wonder if you can riff on this idea that in some cases, throwing software and technology at this is actually the wrong thing to do.

KIP BOYLE 33:32

Yeah. You know, if you ever want a different career, you should call me, because what you just said is completely consistent with our messaging about cyber as a business risk. In any business risk — let's say you've got a sales issue you're working through, or you sell in a foreign currency and you've got to do something to smooth out exchange rate changes — you're generally not going to just throw technology at these things. You're going to come at it more smartly. You're going to say, I need to have a process, I need to know when to buy currency on the foreign exchange and when not to, right? You have to have a smart approach, and you need to set limits. So there's a lot you need to do that has nothing to do with technology.

Now you do still need to include some technology in there, because you want alerting — you want to know when your currency exposures exceed thresholds, and the best way to do that is to set alerts or watch a dashboard. Cyber is the same way. Think about it as: how can I bring as many of the resources I already have at my disposal to bear on this problem? You're going to want to train your folks — that's the people dimension. You're going to want to set policy — tell somebody, hey, if you're going to be on my team, you have to have MFA, it's table stakes. You're going to want to have a good tech stack, of course, but you don't want to go out and buy an obsolete product thinking it's going to cover you, and you also don't want to buy the most expensive thing out there figuring that's an easy button. That's not how it works in my experience. So I absolutely affirm this idea that it's not just a tech problem that you throw tech and money at — that's not going to get you what you need these days.

STEVE 35:45

Necessary but not sufficient, sounds like.

KIP BOYLE 35:48

Yeah. You have to allocate some budget, but don't use it as an easy button or as some kind of substitute for not really digging into this.

STEVE 35:59

Okay. Before we get to the idea of a managed service provider, you mentioned the concept of: you're a busy CEO, you're doing a whole bunch of stuff unrelated to IT security — lean on somebody else. That somebody else could be a fractional Chief Information Security Officer, a full-time in-house hire, a managed service provider, a consultant — any of these things.

KIP BOYLE 36:37

Could be your nephew.

STEVE 36:40

Yeah, could be the smart teenager down the street. At the highest level, how does someone think about which option is most appropriate for them? Because I can put myself in the shoes of someone listening to this saying, great, I understand someone else should be doing this — but who? Full-time, part-time, in-house, outsourced — how should they think about that?

KIP BOYLE 37:03

Right. I would encourage them to think about it the same way they'd think about any business function they need in order to do well — whether it's lead generation, marketing, communications, or subcontractors for order fulfillment. Whatever it is, think about it in that way. And when you do, you need to start with this sense of core competency. If you're a tech company, you might say, I need this in-house — people see us as a tech company and we really can't afford to be seen as incompetent with technology. So I'm going to bring this in-house. Conversely, I've got a customer who does political campaign mailings — you know, when you open your mailbox during election season and get those cardboard flyers of different sizes. Well, tech is not core to who they are to their customers. They use a lot of tech, but it's not core. So they may decide it doesn't make sense to have IT in-house.

Now, the corollary to this is: don't think for a minute that you're not a tech company, because everybody is a tech company. It's just that some are more obviously tech

companies than others. Can I tell you a quick story about that?

STEVE 38:48

Please do.

KIP BOYLE 38:50

I was helping a company in eastern Washington — I'm based in Seattle, and there are so many fruit growers in eastern Washington, a lot of apple growers. I was talking to the CFO of an apple company and having a good conversation, but all of a sudden he got a faraway look on his face. I could see that he sort of checked out on the conversation and I was like, wait, what's going on? Are you okay? Did I say something wrong? And he said, "No, it's just that I can't believe I'm having this conversation with you, because we're just farmers. Why am I dealing with this?"

And so I said, okay, great question. Let me ask you one. Can you put a single piece of fruit into the hands of any of your customers without your computers being on and doing what they're supposed to do? And it took him a minute, but he came back and said, "You're right, I can't." So most every company — whether they've deliberately chosen this or backed into it — is highly dependent on technology to exist. Don't make the mistake of having this identity crisis where you think tech isn't that important.

STEVE 40:06

Yep. That makes sense. So in my experience in the small business ecosystem, a managed service provider is a pretty common solution for small businesses that don't have internal IT — essentially outsourced IT, at the risk of oversimplifying it drastically. Okay, so a CEO might say it makes sense for me to outsource this to an MSP. But even choosing among two, three, or four MSPs can be hard. How do I know what good looks like versus less good? If you were creating a practical rubric for a non-technical CEO evaluating three MSP candidates, what criteria would you be sure to include on that list?

KIP BOYLE 40:53

Well, the first thing is I would want to know if they have experience working with companies like ours — the difference between working with a political mailer organisation where tech is important but not core to who they are, versus maybe an insurtech company. These are tech companies that sell to insurance companies — non-regulated, selling into regulated industries, coding a lot of software, but not wanting to do their own break-fix support. So you want to be really clear about who you are and find an MSP that has worked with similar

companies. I'd say that's the first thing.

Second thing: references. Talk to current customers of any MSP you're considering and ask the hard questions. And third — whichever one you decide to go with — insist on a trial period. It could be 90 days, could be 180 days — it's probably going to take that long to figure out whether it's a good fit or not. But definitely look for some kind of trial period, especially with an escape clause that says if they really mess up, you can stop quickly — say, seven days' notice or something like that. Because here's what I know from talking to all my customers: nobody likes their MSP. Okay. There's always something annoying or not quite right. So don't go into it thinking there's an ideal fit out there. I think you should be looking for a good enough fit — lower your expectations a little bit. I don't think it's because people are behaving badly; it's just the nature of how this works.

STEVE 43:10

So when a company outsources something to a third party, often they grow out of it. For example, let's say I launched a new business and outsourced my bookkeeping. At that point in my company's life cycle, that made perfect sense. But then years later, I have way more customers, way more invoices, way more receivables, and I've just graduated out of an outsourced bookkeeping function and need it in-house. Is there a similar chain of logic with IT and cybersecurity? Is there a point at which you look at your MSP and say, this made sense five years ago, but I've just grown out of it?

KIP BOYLE 43:57

Absolutely, the answer is yes. And I like your example because it makes an important point: a growing company is going to outgrow systems constantly — it could be your CRM, it could be your email service provider. Maybe QuickBooks Online was just fine, but now your financial burden is so tremendous that you do need a bookkeeper. And then eventually you need to raise money and you need a controller or a CFO, but maybe you can't put that person on your team full-time because there's not full-time work yet. You need someone who'll advise and help you but not become a full-time delegate. For IT, it's absolutely the same thing.

So you're going to want to look at options like a fractional Chief Technology Officer, or a fractional Chief Information Officer, or — depending on your situation — a fractional Chief Information Security Officer like me might make a lot of sense, because I have to know not only how to secure systems but how they work. That means I've been asked to wear the fractional CTO and fractional CISO hats simultaneously — sometimes you can put those

two hats on the same person and it can work for a while. But yes, to answer your question, that comes up, and those are some of the ways you can deal with it.

STEVE 45:49

So no conversation in 2026 would be complete without discussing AI. That's where I'd like to go next. Maybe a two-part question: how has your life changed most significantly in 2026 versus, let's say, 2022 before the kind of tsunami of AI hit? And also: how has the risk landscape for small business owners changed over the past four years or so?

KIP BOYLE 46:23

Yeah. Boy, so much to talk about there — but I promise I'm not going to launch into jargon-filled answers. When ChatGPT launched at the end of 2022, I thought: wow, this is so interesting to me. I knew something about AI, something about generative AI, but more in an academic sense. And I thought, to be able to play with this would be really cool. So I've been a daily user of generative AI almost from the beginning of ChatGPT's public existence. And it's made a tremendous impact on me, both personally and at work.

At work, the way I see it: AI is a wonderful augmentation tool. I don't see generative AI as replacing people — although that's clearly something a lot of folks talk about in the popular media. I think about it the way I think about electronic spreadsheets. Before electronic spreadsheets were available, we still had spreadsheets — but they were giant walls with lines on them and people standing there with grease pencils writing numbers into different cells. We still use spreadsheets, but now that they're electronic, they can do so much more than they ever could have done with a grease pencil. That's how I think about AI — I can use artificial intelligence to do the stuff it's absolutely great at: text processing, image processing. But it has to be paired with a human, because the human being has to have judgment — right now, AI doesn't have good judgment.

I tell people all the time that right now, and for the foreseeable future, generative AI should be thought of as an over-eager intern. Have you ever worked with a young person who just wants to make you happy? They're like, I deserve to be here, I'm going to give it everything. Someone else said to me the other day that if that doesn't resonate with you, think of it like a golden retriever: I'll do anything to make you happy, and along the way I'll tip over the lamp and chew on something you wish I hadn't. But I'm all for you. And that's how I've been treating AI. As a result, myself and my team, we're producing higher-quality work than we did before, and we're doing it faster. Productivity is up and quality is up.

In my personal life I've also used it. For example, we wanted to start batch cooking meals to refrigerate for the week. I wasn't great in the kitchen and didn't feel competent. But I thought, maybe this is a good case for AI. I asked my wife to give me some recipes she thought we should make, and I put those recipes into AI and asked how to batch cook them. Now every week for the past six months, I go to it and say: these are the meals I want to eat this week — how can I make them in the least amount of time while still having decent meals? It scales the recipes for the number of servings I want, makes substitutions — I have to stay away from gluten, but not everybody in my family does — and it knows how to recommend substitutes that won't compromise the quality of the meal but will remove the allergen. As a family we're now doing something that everybody actually enjoys eating. It's been wonderful.

STEVE 51:16

I wonder, in terms of the risk landscape for small businesses — if I were an optimist, I would say AI is a net positive for cybersecurity because of more sophisticated detection and remediation tools. And if I were a pessimist, I'd say it's a net negative because it enables more sophisticated tools for deception and attacks and social engineering. So where do you shake out on this? Is AI a net positive or a net negative for cybersecurity, specific to small businesses?

KIP BOYLE 51:50

I think there's a bigger picture I have to reference in order to answer your question. AI is a tool. And any time cyber attackers get their hands on a new tool, they will develop capabilities that cybersecurity people will then have to figure out how to respond to. It's a cat-and-mouse game. And it's been like that for a long time, going back to the 1980s actually. So even though AI is novel — and it is, because it's such a general-purpose technology — it's just the latest in a long line of tools and innovations that have made criminals more capable at what they do, and that we then have to figure out how to catch up with.

I'll give you an example of something that has nothing to do with AI that will help make this point. In the criminal world — loosely what we call the dark web — criminals have borrowed our business models and organised themselves to be highly specialised. If I wanted to launch ransomware attacks, I don't have to be technical. I just have to find someone on the dark web who will sell me a malware license. I give them 30% of every ransom I collect, and I keep 70%. If you can sign up for a Netflix subscription, you can do this. They've borrowed genuine innovations from the business community and used them

to scale themselves and steal more money than ever before.

STEVE 53:49

What role should insurance play — specifically cyber insurance — in an overall protection plan? What do you think it does particularly well, and where do people tend to overestimate the role it can play?

KIP BOYLE 54:05

Yes, you should have cyber insurance, first of all.

STEVE 54:09

It is getting increasingly expensive, and seemingly…

KIP BOYLE 54:13

Yeah. So I should tell you that I have a lot of experience helping companies of all sizes acquire and renew cyber insurance — I sit next to them through the process and I've seen all kinds of interesting things. One thing I want to share is that the difficulty of getting cyber insurance and the amount you'll pay for a policy goes up and down over time. Right now, as we record this, the market for cyber insurance is considered to be soft, which means it's relatively easy to get coverage. But about two or three years ago, the market was hard — difficult to get coverage, and expensive if you could. The reason goes back to what I was saying before: cyber is a dynamic risk. When insurance companies crunch all the data about who's getting hacked and figure out, okay, everyone's getting hacked because MFA has become weak, they require everybody to up their game, and their losses go down. Then the cyber criminals innovate, that control becomes less effective, and losses start to go up again. So you get this porpoising effect. Just because cyber insurance is soft today doesn't mean it will stay that way, and it will get hard again.

So how do you deal with this? You have to go get a broker who specialises in cyber liability insurance. Whoever you're buying your E&O; policy or your general liability from today may not be the best person to help you choose a cyber product, because cyber is non-standard. Every carrier is offering a different policy with different subjectivities, different exclusions, different retention rates — it's very difficult to compare them. But if you get an independent broker, they can make it apples to apples and help make sure you get great coverage for the right price.

STEVE 58:04

Where do you stand on passkeys? Because I know a lot of technology providers are pushing this as a more secure alternative to passwords. And you mentioned stolen passwords as one of the primary vulnerabilities. Does this strike you as a helpful and constructive point of progress? Is it overhyped? I'd just like to hear your opinion on them.

KIP BOYLE 58:28

Yeah. Like a lot of things, it's a little of both. First of all, we have to get really clear on what a passkey is, because I think there's some confusion. Some people are under the impression that if they put their email address into a web form, click log in, get a code by email, copy that code into the form, and get in — well, some people call that a passkey because there's no traditional password. But that's not a passkey in the sense that I think you're using the term. A genuine passkey involves encryption and is way more sophisticated than just getting a six-digit code by email — which is really just another form of getting it by text message, minus the password. So in a way, they've sort of co-opted this idea of a passkey to get rid of passwords, but it's nowhere near as strong as a genuine passkey. That's the hype, that's the misunderstanding.

But passkeys in the genuine sense are very, very good — I really support them. There are many different types. A passkey could be a physical key that you plug into your computer's USB port. It can also be a key that you tap on your phone, like using Apple Pay or Google Pay to do a tap-to-pay transaction. Those are real passkeys, and I think they're a great innovation. The problem right now with real passkeys, though, is interoperability. If I use a passkey for my Google login, how do I know it's going to work at my bank? And if it does work at my bank while I'm sitting at my computer at home, can I use it with my iPhone when I'm on the road to get to the same bank account? That's not sorted out yet. So we have to be really careful about using passkeys and making assumptions about all the places they will work, because I'm not seeing high levels of interoperability yet.

STEVE 1:01:07

Let's get back to the human side, because again, a CEO can throw a lot of money and time and technology at this problem. But if some employee doesn't take it seriously and flippantly clicks on something they shouldn't, that in and of itself is a very meaningful point of vulnerability. So I'm curious — in the companies you've worked with, what are some of the best ways you've seen leaders train employees on good cybersecurity hygiene and really communicate its importance?

KIP BOYLE 1:01:44

The underlying success factor, no matter how you do it, is clear to me: tone at the top. If you're the business owner — or if you've hired a CEO — that person has to talk the talk and walk the walk. If they don't, nobody will take it seriously. So that's the first thing: if you're the owner and you're saying "MFA for everybody except me," it isn't going to work. Because that's just human nature — people are not going to inconvenience themselves if you're not willing to get into that inconvenience yourself. If you don't do that, you're going to get uneven results no matter what you try.

But let's say you're good with that. Let's say you're okay with turning on MFA and doing all the things you ask your folks to do. Great. Here's step number two: psychological safety. If somebody clicks on something they shouldn't have clicked on, they have to feel like they can tell somebody they made a mistake without worrying about being disciplined or fired for it. I've worked in many organizations perceived to be "one mistake" workplaces, and I've seen a lot of stuff get covered over because people were afraid to admit they had made a mistake.

STEVE 1:03:29
Yeah, that makes sense.

KIP BOYLE 1:03:30
That results in a lot of damage.

STEVE 1:03:34
That makes sense. What about ongoing training? I know that's a thing. I can't remember — I think the tool is called KnowBe4. Maybe I'm making that up.

KIP BOYLE 1:03:44
That's a very popular one.

STEVE 1:03:45
Yeah, they basically send what I'll kind of imperfectly refer to as fake emails, just to see if employees actually click on these things.

KIP BOYLE 1:03:56
Right.

STEVE 1:03:57

Right. Where do you stand on the usefulness of those types of things as tools? Other companies will do quizzes or surveys that people have to fill out every quarter, for example.

KIP BOYLE 1:04:11

They have a lot of potential as a category. What I see a lot of people do is use them in a more performative way. In other words: I have a requirement to train my people — maybe that comes from a regulator, maybe from a customer — so they'll get a subscription to a service like KnowBe4, use it in its default configuration, check the box, and get on with their day. Now that's the functional equivalent of what we talked about earlier: throwing technology and money at a problem and ignoring the people, process, and policy aspects of it. Because there have been so many scandals — not just in the cybersecurity space — about people who have to take mandatory training where they have it running on a second monitor.

STEVE 1:05:15

Yeah, of course.

KIP BOYLE 1:05:16

...and don't pay attention to it. Yeah. Because they just want that checkbox.

STEVE 1:05:20

I would imagine that's the default.

KIP BOYLE 1:05:22

Yeah. Because they know this thing isn't serious — the tone at the top sent no signal that it was serious. It's just a thing I have to do to continue to collect my paycheck. So that's where those tools are not very helpful. Are they going to let you check that box? Yes. Are they actually going to make a difference in your actual risk that you face every day when you open for business? Probably not.

So where you want to use ongoing training or testing is with full disclosure, and making it as meaningful as possible. Instead of having people watch a generic cybersecurity video that has nothing to do with your organization, you might just want to make a five-minute video, post it on YouTube as an unlisted video, and just say what you want your team to know — then require people to watch it at an all-hands meeting or something like that. That's going to have more effect on your folks doing the right thing than just about anything else I can suggest.

Now, on the testing side: there are a lot of really awful stories in the news about phishing tests gone wrong. Have you ever seen them?

STEVE 1:07:06

Hmm, I don't think so, no.

KIP BOYLE 1:07:07

So I'll give you a good example. The people in IT who typically run these things will sometimes send out emails where their goal is to catch people doing bad things and punish them. It's a very punitive approach. So they'll send out emails like, "Hey everybody, the company has just declared a big bonus — click here to tell us where you want your money deposited," and people get excited. But it was a trap. And when you run your test programme that way, all you're really doing is frustrating people and eroding their confidence and trust in management. You don't want that.

The better way to do it is to tell people upfront: hey, we send these phishing test emails out. We're not testing you — we're testing the controls we use to keep these things out of your inbox. So if you see one, just report it. And if you click on one, nobody's going to get in trouble — we just want to have a conversation about why you clicked it, because that'll help us do a better job of keeping this stuff from showing up in the future. Do you see the difference?

STEVE 1:08:32

Remote work and purely remote companies are certainly more common today than they were five or six years ago. If you were advising two otherwise identical companies, but company A was 100 percent in-office and company B was 100 percent remote — are there any major differences in how you would work with them? Major points of vulnerability, major strategic decisions? What really differs between the two?

KIP BOYLE 1:09:00

I work with companies that range across all of those categories — fully in-office, fully remote, and hybrid. There's actually some advantages to being a fully remote organisation, and some disadvantages to being what I'd call a legacy organisation where everybody works in an office building. And I should let you know that my company is all remote, all virtual — so I'm speaking from experience, not just from working with customers.

If you're all remote, there's no local area network, there's no central place to attack. A lot of cyber attacks happen against companies that have legacy networks because they can be pretty easy to exploit if they're not buttoned down really, really well. If you're a cloud-first company with no legacy hardware, no legacy local area networks, fully distributed and fully remote, then the question for an attacker becomes: how do I attack that? It's not as obvious. Not to say it can't be done — it's just different. If I can get Kip's account, for example, then I can do a lot of damage. I can get Kip's bookkeeper to send money somewhere in a business email compromise. It just requires a little bit more effort, but it's different. So the big takeaway from your question is: how you protect yourself is going to vary depending on whether you're a traditional in-office organisation, a hybrid, or fully remote — and whether you're cloud-first, cloud-exclusive, or hybrid. There are nuances to each one of those situations that you need to pay attention to.

STEVE 1:11:26

Okay, so let's put ourselves in the uncomfortable position of the nuclear scenario. Let's imagine a CEO learns tomorrow that their company has suffered some sort of serious breach. What should they definitely do during the first hour, first day, first week? And conversely, what should they definitely not do during that period of time?

KIP BOYLE 1:11:49

Okay, so in the first hour, the most important thing is: try not to panic. That's really easy for me to say, but if you don't have a plan that you've rehearsed, you're probably going to panic — because the adrenaline is going to dump into your blood, the cortisol, everything, and you're going to feel more alive than you've felt in months because everything you've built is at risk. I get that. But when you let your lizard brain — the amygdala, the centre of the fight-or-flight response in our primitive brain — when you let that thing take over and you keep feeding it caffeine and energy drinks, that's not a good place to be. Because when that part of your brain activates, it actually shuts off your prefrontal cortex — which is the part that makes sound, rational decisions. This is the part you want on when you're in a situation that might be the fight of your life, certainly the fight of your firm.

So: don't panic. And don't destroy evidence. If you've got a machine that's infected with ransomware or something like that, don't just wipe that machine and reload it to get Joe back on task. I understand that's the instinct — that's kind of the muscle memory from 15 or 20 years ago. But don't do it, because without that evidence, it may be very difficult to figure out how to recover. The malware these days is just so much more sophisticated. Don't panic and don't destroy evidence.

Your very next move is to call your incident response team. If you have a cyber insurance policy, call them. One of the wonderful things about cyber insurance is that the team of people you want to call in an incident are on retainer with your insurance company at preferred rates. And it's not like calling your auto insurance company, where you're afraid your rates will get jacked up — cyber insurance doesn't quite work that way. But call them, because they'll give you a data breach coach, they'll send a digital forensics team to get that evidence, and you'll be put in touch with an attorney who can help you figure out whether you have legal liabilities, whether you'll have to report to regulators, and whether you'll have to send notifications.

My more sophisticated customers have outside counsel on retainer, because when they call me and say "we think we've been hacked," I can work through that outside attorney — and all the work we do becomes attorney-client privileged. Which means that if records ever get requested because there's a lawsuit or a regulatory investigation, those records are privileged and you don't have to just hand them right over. So that's a very good place to be. Then let the insurance company help you and guide you through that first hour when you're probably panicking. Let them help you.

STEVE 1:15:44

I think that's a great place to start. So: in our first hour, we've resisted the temptation to panic, we've contacted our insurance provider, we have not wiped the evidence. Let's say the proverbial lights are still on and the sky has not fallen on the first day. Now we're on day two, three, four, five — what does that look like?

KIP BOYLE 1:16:06

You might just be in the afternoon of the first day, depending…

STEVE 1:16:09

Or maybe it feels like day five, but it's actually hour five.

KIP BOYLE 1:16:12

Yeah. Yeah, exactly.

STEVE 1:16:14

What do those next couple of days look like from a best-practice standpoint?

KIP BOYLE 1:16:19

A big priority is going to be containment and eradication. Containment means: if it's ransomware, can you keep it from spreading to other systems that it hasn't reached yet? Research tells us that the more containment you can get on an incident like that, the lower the cost is going to be to clean up and recover. Eradication is next — you want whoever's attacking you out of your systems. Because if you think they're out but they're not really out, you'll rebuild and they'll still be in there. Just when you think you're going to emerge from this nightmare, they can pop you again and you'll be right back in it. So nobody wants that.

You're also going to want to take notes. Everything that you talk to somebody about, write it down. Called the insurance company on this date, at this time, told them I need help and may have a breach. You don't need to write a diary, but you do need to keep a written record of the major things that are happening, because that's going to become evidence later on. Depending on how bad this is, you may need to show an attorney, a regulator, or your biggest customer exactly what you did — to demonstrate that you were behaving reasonably. Nobody expects perfect cybersecurity these days. The Federal Trade Commission has been on record for over 20 years: they don't think there is such a thing as perfect cybersecurity. They just want to see us behave reasonably. So that's where this advice is coming from — don't try to be perfect, just try to be reasonable.

You also don't want to go public with this stuff until you know what's going on. If you're a consumer-facing organisation with a high profile, you need to spin up your PR team, your external comms team, and your internal comms team — because you are going to run into reputational issues if the word gets out that you've been hacked but nobody knows anything about it. People will always assume the worst. So if you're a sophisticated risk manager, your comms team already has holding statements ready: telling employees not to take a picture of the ransomware note on their screen and post it on social media; and telling reporters or anyone who calls that we have an incident, we're working it, we're aware of it, and we'll keep you updated. Make sure you control those comms and say what you need to say when you need to say it.

And when the digital forensics people and support team show up from your insurance carrier — follow their instructions. They're going to be more clinical about this than you can probably be. Trust them as much as you can and follow their advice.

STEVE 1:20:31

Let me take you into a hypothetical but ultimately extremely realistic scenario for the folks listening to this. Let's say you were planning to buy a small business and everything's checking out — you like the product, you like the market, you like the team, you're otherwise very happy. However, you've noticed the company has little to no IT strategy, no team, no documentation, and cybersecurity just feels like a real hole. There haven't been attacks in the past, but there's really nothing there to prevent one in the future. As a potential acquirer, how do you think about that? Is it a deal killer? Is it a big value-creation opportunity? Is it somewhere in the middle?

KIP BOYLE 1:21:21

Well, the first thing I recommend to somebody in that situation is: if you've ever bought a home for your personal residence, there's some conceptual similarity. If you buy real estate sight unseen in a frothy market — because you're concerned about getting outbid — you're going to skip things like the whole-home inspection. You might have looked at the photos, walked through it once, and smelled the fresh paint. But do you have a cracked foundation? Are there termites in the walls? Are the joists in your roof rotted out and ready to crumble? You haven't checked all that stuff. This is what you need to think about when purchasing a company, because bad cybersecurity problems can hide — like a cracked foundation, like termites, like rotted joists — because you don't see them when you're just in there shaking hands and looking at the books. So you have to do your due diligence. You have to really get in there and maybe do some testing to find out if there's anything hiding in that company's infrastructure.

And I wouldn't be surprised if there was, because here's something we see all the time. A business email compromise — where somebody intercepts a purchase request or an invoice and changes the bank account information, so you pay it but you've accidentally sent the money to the attacker's bank account — those attacks don't happen on a purely opportunistic basis. Typically you've been surveilled, they've conducted reconnaissance on you for days, weeks, or months, depending on how big of a target you are. And often what they'll do is sneak into your systems and install virtual devices — in other words, they'll do what you do when you connect your iPhone or Android to Microsoft 365 so you can see your email on your device. They'll do that with phantom virtual devices and then reroute your email so they can send and receive email in your name without you knowing it. That's very difficult to detect. And if you're buying an organisation where that kind of attack is ongoing during the acquisition process, you could end up owning that problem after you become the owner — the trap might be sprung right after you take ownership, even though the attack has been in process for several weeks before the ownership changed.

STEVE 1:24:24

So many of the businesses that we buy are run by their original founders. And in many cases, founders have run these businesses for 10, 20, or 30 years. One of the practical implications of that is that these owners are often in their 60s or 70s. And an owner in her 70s would be forgiven for not investing in the bleeding edge of cybersecurity. So if you look at a company that basically has nothing, as the new owner, are you focusing on the basic cybersecurity stack we talked about at the beginning — getting MFA in, getting antivirus in, getting an endpoint detection system in? Is that how you're spending your first couple of days, weeks, or months from an IT security perspective?

KIP BOYLE 1:25:14

I think so. If you're not a sophisticated buyer and you don't know what else to do, but you've decided to make it a priority — because cyber risk can be existential, and United Structures of America is kind of my poster child for a company that got cyber-attacked and went out of business — yes, those are the things I think you should be focusing on right away. Making sure those basic capabilities are in place, and testing to make sure they actually work.

STEVE 1:25:53

Kip, as we look to land the plane here, I'd be curious to ask you the question that I often try to conclude with: what is the most meaningful lesson that you've learned in your life, across any domain of your life, over the past twelve months?

KIP BOYLE 1:26:11

There's a book I've recently read — a little earlier this year. I read a lot of books. I love learning from other people's mistakes and other people's research. Anyway, the book is called *10x Is Easier Than 2x*.

STEVE 1:26:35

Yeah. Is that Dan Sullivan?

KIP BOYLE 1:26:38

I think it's Dan Sullivan.

STEVE 1:26:39

Dan Sullivan, Dan Sullivan — that's what I meant to say, yep.

KIP BOYLE 1:26:42

Yeah. And he has a co-author, Benjamin Hardy. And it really changes the way I think about how I go about accomplishing my goals. To give a thumbnail sketch of what I learned: the title, *10x Is Easier Than 2x* — well, 2x thinking in this book means I'm just going to grind harder than anyone else at everything I think I need to do to be successful. And if you're an entrepreneur, you know, you just look around and think: I'm just going to grind this stuff out and be better. But 10x thinking is different. It's more thoughtful. It's sitting back and saying: I don't think the answer is grinding on everything — I think there are a few key bets I need to make and go all in on them. And if I'm wise and I've chosen the right critical success factors, I'm going to drop the rest of them, because I can out-earn my way past all these other little fires that aren't getting enough attention.

A good example: I'm so busy trying to get my next product dialed in to achieve product-market fit as soon as possible that I forgot to file my quarterly excise tax. Who cares? Pay the penalty and keep going. Nobody likes to spend money on a penalty because they failed to file a tax report, but don't get it twisted — it's way more important that you get the product-market fit thing figured out than that you're hovering over reporting deadlines. That's not a critical success factor. I hope my attempt to explain my takeaway from the book was clear.

STEVE 1:29:03

Makes sense. The small number of things that actually matter is something that is very relevant both for myself and for those listening. Speaking of those listening, Kip, knowing who you are speaking to — anything left unsaid from today's conversation? Any asks, any offers, anything you want our audience to leave with?

KIP BOYLE 1:29:25

Yeah, absolutely. I told you I have a book — it's called *Fire Doesn't Innovate*. And I would love to offer your entire audience a free PDF version. I'll share the URL with you, Steve, and you can place it in the show notes. I'd be pleased to share it with anyone who'd like to access it. And if you have any questions about anything in there, you're welcome to send me an email — I'd be glad to talk with you about it.

I go to market as an educator. That means I really like talking to people who are interested in this space and sharing what I know. I remember at the top of the show I said I'm in business because I want to make impact — I want to help other people move the needle. And I think it's completely wrong that criminals from other parts of the world can reach into

our economy and steal our legacy from us. If you're building a business as a legacy for your family, or you're building it because you want to serve your customers, it's morally wrong to get attacked by a cyber criminal. It's an awful thing that's happening. And I want to be part of the answer. I want to be part of the solution. I want to protect what people are working so hard to build. So I would love to talk with anybody.

STEVE 1:31:05

What a great place to leave it, and what a generous offer that we will indeed include in the show notes. Kip Boyle, thank you very much for your time. We enjoyed speaking with you today.

KIP BOYLE 1:31:13

You're welcome, Steve.