Martin Hinton (00:05)
Hi, welcome to the next episode of the Cyber Insurance News and Information Podcast. I'm your host and the executive editor of Cyber Insurance News, Martin Hinton. And today joining us, we've got Dan Candee, the CEO of

Cork Protection. ~ What does all that mean? As I'm famous for saying now, I'm going to let Dan tell you because he's going to put it better than I. Dan, first of all, thanks so much for joining us. Really do appreciate you taking the time out today. ~ Tell us a little bit about yourself, how you got to this point in your career, and then tell us a little bit about what

what Cork Protection is.

Dan (00:36)
Yeah, you bet. Thanks for having me today, Marty. It's really nice to say hello. ~ Dan Candee, CEO of Cork Protection. And my journey to this point in my career, I guess, starts when I was 20. And I successfully

out of college to start my first business. And I had been spending some time traveling the world and studying abroad and doing various things. And I realized

I actually wanted to do some more of it. And so I started back to Boulder, Colorado and started a house painting company. And it was at that point that I, ~ you know, realized what it took to make a business work. Eventually I went and finished my undergrad and did some graduate work and got into technology and have built a few businesses over the

and supported a lot of SMB. And ~ eventually I... ~

because of all the time I spent in building software businesses, I ended up over at Dell and I helped build the VMware business and then I got recruited by AWS and I built the VMware cloud and AWS business. And that first week when I was at AWS back then, before COVID, we would go to Seattle. And I remember being in a meeting with Andy Jassy who was then the CEO of AWS.

At one point, he got asked a question, hey, what are some of the cool new services that are coming out for AWS? And he said, actually, there's plenty, but I don't want to talk about that. I want to talk about cybersecurity. And I want to talk about security being job zero. And every day that you come to work at AWS, you need to think about security.

And that really surprised me and has never left my brain. And so when it was time for me to leave AWS, the thing I wanted to focus on was

cybersecurity for Main Street. I've been witnessing and working with Wall Street when I was in the enterprise and they're just fine. But, you my parents own a restaurant. ~

My brother's a police officer.

sister runs nursing facilities. And I myself had built a number of different small businesses. And this is where my heart has always been. And so that's how I ended up here at Cork. And Cork is an absolutely fascinating company. And we've been having a blast because our value proposition is very simple and very unique. And it's that we believe that

small and mid-sized businesses are underwhelmed and underserved when it comes to

modern cybersecurity. What I mean by that is the threat actors are getting better and the threat actors are coming after Main Street more and more. And yet, and there's a lot of cybersecurity solutions.

And I believe that managed service providers are getting better at serving ~ SMB worldwide. But what's happening is there's not a lot of financial Protection ~ that is helping them in the short term. And if your average SMB has 18 days of cash flow in order to maintain, there's a gap.

There's a gap between what cyber insurance can do and the needs of everyday business owners. so Cork was founded on the promise that we can leverage

We can leverage an inside out platform to work with managed service providers and work with SMB so that we can understand where the threat actors are most likely to attack and be able to close some of those doors. And when they do attack, Cork can show up and write checks because we offer

financial Protection and we work very closely with cyber insurance to make sure that they're able to also do their job. And so we've tried to create this holistic environment between technology, people, business and financial Protection in order to keep SMB running every day.

Martin Hinton (04:47)
You

touched on something. You said a word that is, ~ it triggers. You said main street And one of the things that I've encountered in the work I've done on this subject as a journalist is what I've called a few times before, sort of a teenage

amongst small business owners and medium-sized business owners, that this isn't a problem that really affects them. And then when it does, to your point about 18 days of cashflow and a business interruption any longer than that, and you've got a serious existential threat to your existence,

I wonder is it hyperbolic or an exaggeration to say that the small business owners specifically and even medium-sized business owners who are paying attention to this who can't answer the question Do you have ransomware are in in a desperate situation potentially within minutes or days of this moment, right? So if you ask a small business owner What's your deductible on ransomware and they look at you like you're asking them to fly them to moon. That's a problem, right? They have a problem.

that fair?

Dan (05:45)
It It is, and I am not an

fear-mongering type of guy, right?

I want to approach every single conversation with education. And so when you ask me that question, I go back to the data that I

across all of my partners and all of my clients. And so if I think of the snapshot, the last 12 months, we've witnessed 2.3, 2.3 something million compliance events across about a half a million of endpoints.

When I think about the volume and velocity of those compliance events ~ and what's happening, the rate at which they're happening for small business and where they are happening, it really scares me.

the types of situations where managed service providers in Cork are coming to help, where I'm literally writing checks and paying out on warranties and working with insurance companies to make sure that we're helping our customers in those

It's frequently these sub $50,000 hits that are ACH wire transfer frauds, right?

mini ransomwares, right? It's a lot of these fast and little ones. And so, and that's enough pain, right?

put small businesses just on tilt. ~ And it's becoming more frequent.

Does that help at all?

Martin Hinton (07:22)
Yeah, no, I think you touch on something that

I think that, you know, we hear a lot about the new new thing. So AI is the new thing and we can get into that in a little bit. But the idea that there's a death by a thousand tiny cuts kind of thing for these companies and

the scale and you know, if you think if you take ransomware as a service, right, you know, I think most people probably know, maybe they don't, who knows, but we'll say it just to be sure. You don't have to be a computer expert to be a criminal

the cyber world anymore, right?

The idea is that anyone can steal a car or break into a house. You just have to be motivated by the desire to steal something of value. And that is so easy now. And I mean, you think about, you just touched on it, the wire transfer fraud and the business email compromise. I wonder if you could just explain those a little bit for me so that I've got it down, if you will. We saw this with the Spencer hack, or maybe it was one of the other hacks there, but someone called the IT department.

Convince them to reset a password. I that's old-school street level con stuff There's no there's no computer programming going on there and I think that that's where I think people think

you know Why would anyone steal my data? Well, if you're wiring out 400 grand in a month or you're receiving payments and they can compromise just 5 % of that across a thousand companies That's a huge payday. Go ahead

Dan (08:44)
Yeah, two things. I myself was surprised when I learned last year that there's essentially an illegal eBay where threat actors can go on and just buy and bid on anybody's credentials and information. Cheap, right? So to think that all of

information is that accessible today, right? That means that volumes of people worldwide

can simply purchase, consume, put into their tools, leverage some AI, and begin going after us, it's a little frightening. I don't like that at all. And so that's how easy it is for threat actors to do it. And then on the flip side of this, I'm also happy that things like the nationwide toll scam is going on.

Of course, it's a horrible thing that it's happening, but it raises the awareness to people because it's such a simple thing so that everybody understands. Wow. It's simple things such as my telephone number.

is making, you know, we're all so vulnerable and at risk right now. And so if

Martin Hinton (10:01)
Yeah.

Dan (10:03)
else, there is awareness. Okay. And then to give you sorry, did you want to say something? Because I really want to give you a real. Okay. So this is a real example that we have been involved in with one of our partners.

Martin Hinton (10:07)
No, no, you're going, keep going, ahead. I'll remember what I was gonna say. Go ahead.

Dan (10:17)
And this is a relatively common thing that we are seeing with small businesses. ACH wire transfer

is on the rise. And what's happening, according to the data that we're seeing, is about 88 % of the payouts that we're responsible for. It's because of human error associated with the tricks that the threat actors are doing.

And so in this most recent one, and we've published a success story on it or a case study on it a couple of weeks ago. So Canadian partner of ours taking care of a construction company. Excellent partner, been in business for almost 30 years, leveraging Sentinel-1, Ninja, and FEMA for...

~ education, right, like a lot of great technology in order to support this particular client.

And what happened was the threat actors got into the architecture firm that supports this particular construction company.

And they figured out who at the construction company sends the ACH payments. And they sent three emails to three different people saying, hey, the wire, the number has changed. Please send your money to this new one. And that's pretty sophisticated, pretty smart, kind of a supply chain attack, right? And so the construction company.

you know, everything was protected, everything made sense. The only thing they didn't do was pick up the phone to verify, hey, is this really true? That would have been a great step to do. But they sent the money and, you know, ultimately they didn't realize what had happened until the architecture firm had asked for their $21,000.

Martin Hinton (12:05)
I mean the-

tale there is trust but verify, right? Do not, you know, and one of the things that's interesting in this day and age where people don't make

calls like they used to is that there is a social engineering element to that where you take advantage of the email and people think email is this great tool, which it is, but it's also very, very vulnerable to this sort of manipulation. And as a result of our reliance on it, so are we. So it is a

in that tale that

If you get one of these emails saying someone's changed their banking information, you need to have a, I dare say, second authentication step before you go ahead and just wire the money to a totally different account.

Dan (12:44)
Yeah, absolutely. ~ If something smells a little off, ~ then you should definitely take that extra step. Look, in this particular case, the company had a great service provider to work with. They were being managed really well with good technology. And there was some good protocol. But there's always that next step. And so in the spirit of continuously learning,

continuously learning,

as business owners, it's our obligation.

to figure out how can we learn, how can we stay abreast of the next level of thinking. And we ask, you know, ~ we have to work with the people in order to understand how we can do that in the business. And as a technology owner, right, now as I learn from these things, now I work with my partners and other technology companies to add these extra levels of gates and

Martin Hinton (13:44)
You.

Dan (13:44)
them. So look, at the end of the day,

~ human error occurs and it will always occur and we'll keep leveraging technology to close some of those doors.

But that's the key. That's what makes court Protection so unique. And that's why we created because it's why we're so differentiated. We're

managing the compliance risk because we have this inside out technology, much like a CT scan, right? If you go to the cardiologist, we're able to predict, Hey, there you're actually at risk for stroke because there's some clots here. We do that in an

agentless fashion because we believe in the modern world, there's so many great

technology companies. And so we believe the managed service providers can choose the best of breed technologies that are out there. So we invest in the MSPs and we invest in companies like Roost to do automation, to speed up the way that we can close these doors. So today we cover 93 % of the market with all of these integrations and then less than an hour and for less than a dollar an endpoint managed service provider

can see the entire ecosystem for all of their clients. And so we're able to help them be 77 % 77 % compliant in just a simple week. And together we're working to protect Main Street. At the end of the day, there's still that financial piece. And I believe that cybersecurity insurance companies are trying to get there as well. And they really do, you know, I think there's, when it comes to some of writing the bigger checks and

and paying for some of the more complex types of things associated with a breach. ~

I think there's so much value there. And what I found that between our short-term impact, where I have an SLA, within one hour I'm over a $10,000 electronic credit card to my partners, within 14 days, I'm reimbursing the client and the partner for their out-of-pocket expenses back to that 18-day cash flow piece. So I'm there in the short term, and I can work with the insurance companies on the long term. And together, we keep businesses.

Martin Hinton (15:59)
That pace of resilience, right? Bringing that help quicker than say a normal insurance environment, that's for small businesses in a financial situation. Again, we talk about the 18 day cashflow thing. These are the sorts of things that make the difference between survival and extinction, right? And is that one of the elements of the cyber insurance, cybersecurity insurance world that needs to be a bit more nimble given how

Dan (16:21)
Absolutely.

Martin Hinton (16:26)
devastating these attacks can be ~ to particularly small businesses.

Dan (16:31)
I believe so. ~ We are backed. ~ We have our own insurance captive. We work very closely with insurance companies, right, because we have to be prepared to pay out ~ ourselves. So we understand the insurance business fairly well. And so, yes,

you know, we're built for speed and in order to complement one another. So I see a lot of progress in the world.

But at the end of the day, my business is to serve the SMB market. And that service mindset means who is providing the most value fastest. And I believe in managed service providers, MSPs and MSSP's, who are truly doing the most amount of work worldwide. so when I think of that,

I'm constantly trying to figure out how can I help them save time and be more efficient. So that's why we recently released our cyber insurance analyzer. And the funny thing about this one is, over the last year and a half or so, our partners were bringing us their clients' cyber insurance policies and saying, hey, can you help take a look at this? So obviously, managed service providers do not sell cyber insurance. I don't sell cyber insurance.

But we're involved in the technology side, right? Because we can see every single endpoint and we're involved in all of those long checklists and all of the things. We have an active dashboard, so it's all automated on our side. So we're automatically saving time. Well, the individual on our team who was doing all of those, she went on maternity leave. And so it fell on the rest of our team and we thought there's got to be a better way to do this. ~

And so we leveraged some agentic AI we happen to be working on

different project and we automated built it into our platform. And now it's a drag and drop for our partners who will just pop in the clients, cybersecurity, insurance.

And it will pop out a summary,

facing with a general risk analysis and some insights and where there's potential lacking coverage, some highlights, some lowlights that allow them to have an informed opinion. And if there's an opportunity for short-term coverage where court can be of service, it talks about that as well. And then we're tied into various cyber insurance brokers because that's where the brokers these days, especially those focused

and cyber insurance, they're the thought leaders, they're the experts who actually are working with the 50, 60

out there who are doing a really good job supporting the clients. And so we're able to very quickly, we've created the easy button for MSPs and clients to have both warranty and insurance and get the right coverage and be on that journey.

Martin Hinton (19:17)
You.

So

I am not a cyber security or insurance expert, nevermind insurance, I'm a journalist. And one of the things that when I started to dig into this work, I...

~ Complexity to the lingo a lot of acronyms and a lot of phrases and the financial part of insurance and reinsurance is very very complicated You You talk about the analyzer the drag-and-drop element of it all there must be a real sense of clarity like I have a jokey sort of segment I do on the website where it's the explain it to me like I'm a fifth grader right because

I'm trying to run a dry cleaning business or a small law firm and I've got lots of really complicated things going on. I don't understand how my fire insurance works or my indemnity insurance works. This is a whole new thing. What's the reaction been to the, is there an aha moment for the clients?

Dan (20:29)
It has been absolutely bonkers because it is one of the most complex and time consuming things and we have taken it from hours or days down to less than two minutes.

And to be able to take these very interesting documents and to create a one pager, right? And then that one pager into a three pager and to be able to consume it and have those talking points and then be able to actually take some action and have a more intelligent conversation with your cyber insurance broker. Clients and partners now feel empowered to understand what they have and what they don't have.

because

It's one thing to anticipate, but it's always the fear of when things go sideways, who's going to be there with me? And knowing that beforehand is the confidence. So I'm in the trust business, right? I have to be there when people need me. And so being able to offer that trust beforehand and then be there at that moment, that's what we do day in and day out. And so this tool, which is free, ~ helps set the clients

for success in that particular fashion. It's kind of funny we we keep

getting asked if we can just if they can just license if other people can license or have the tool and I'd love to get to a point where I can just give it away for free. Whatever we can do to help.

Martin Hinton (22:04)
Obviously, you've explained how we use it to analyze the policies for cyber insurance to help break down some of the complex language and make it something that people like me can understand. AI more broadly, and we're starting to see the phrase agentic AI, which means it has agency over itself. I wonder if you could tell me a little about how you see that now and how fast you see it evolving.

~ as a tool for protecting people.

Dan (22:29)
Yeah, you bet.

We leveraged agentic AI when we were building this one, which is really creating a number of frameworks that it operates within to give us an informed opinion that we based upon the rules that we had asked for. And so the point of that is to expedite particular knowledge base outputs, right? At the end of the day, these are learning models. And in our case, like in most technology companies,

These are simply useful tools. And for our managed service providers and most business owners, the utility is not in and not.

the AI itself, it's the output of businesses like mine. When technology companies leverage those tools to create efficiencies for SMB so that they can run their mission better and without as much distraction, I see that's where the successful point is. The restaurant needs to serve better, more delicious food more consistently.

need to be thinking about AI. But if the tools and the services can protect that business and or deliver the things needed for that particular restaurant more quickly and less expensively, great. And AI can play a component in all of that, whether it's the accounting systems or the delivery of the food and reducing the cost. There's lots of those types of examples. The problem is when it comes to cybersecurity,

threat actors are really organized businesses, right? Even when they're in foreign states. These are not necessarily people in hoodies in basements, you know, who are just kind of one-offs. Plenty of those exist. When we're looking at the volume and level of sophistication that's really beginning to shift from the enterprise,

towards SMB. That's what concerns me because the utilization of AI and those tools in order to create the sophisticated threats is beginning

to accelerate. And that's where it's the obligation of all of the cybersecurity technology companies out there to do better.

The interesting part of all of this and the one that is the obligation of the cybersecurity technology companies is to understand how the threat actors are leveraging AI and all of the advanced tooling in order to get better at coming after Main Street. And that's what really concerns me.

because just like the good guys, the bad guys and the bad gals are doing the same thing. And it's good to see so many consortiums of thought leadership across the 6,500 cybersecurity solutions these days, according to the most recent Canalys study. So there's a lot of great solutions and they're working together more and more.

in order to create levels of compliance that really matters around SMB. ~

Martin Hinton (25:57)
used a few acronyms and I know what they mean, but I wonder

just for the audience, I might peel this off as a standalone because I think a lot of people, I don't mean to be silly, but things like MSP and MSSP, what does that mean and what do they do?

Dan (26:14)
You bet. IT service providers and managed service providers, or managed security service providers, are the organizations around the world that work with businesses to bring a variety of different services to help small, mid-size, large businesses succeed. Everything from providing the hardware to supporting all of the cloud services.

everything that's needed for most modern businesses to be able to deliver their own services to their clients. so Cork is very focused on supporting managed service providers

Martin Hinton (26:58)
managed service providers,

Dan (26:59)
We believe...

Martin Hinton (27:00)
basically

that's like having an out of house law firm or the accounting department. It's someone who handles the technical part of things in a way that those types of companies might handle your bookkeeping or your tax returns, right? It's not some crazy, confusing, scary new thing. It's part of the supply chain of how small businesses work.

Dan (27:21)
Absolutely. Just like if you're not a mechanic and you need some help with your car, you take your car to the mechanic. When it's tax time, you call up your accountant and make sure that they're helping you. Well, it's the same thing with modern technology for your business. You need to make sure that you've got the right professionals helping you with the variety of different services that are out there.

When it comes to cybersecurity, today's managed service providers understand how to protect your devices, how to protect your data, how to protect your brand reputation, and they know how to work with all of the various tech companies that exist out there, companies like mine. ~

to really keep you as safe, secure as possible and really to allow you to empower you, the business owner,

Martin Hinton (28:13)
You,

Dan (28:14)
to focus on taking care of your clients.

Martin Hinton (28:14)
we touched on the beginning. If

you're a small business owner and you've seen some of this podcast and maybe you've thought, whoa, I don't know whether I'm covered for ransomware. What's their first step? What do they do next? Give them a playbook for how to address the fact that they just realized, I don't even know if I'm cyber resilient. I don't even know what that means. What should they do?

Dan (28:36)
One of the first things to think about is, I guess I would put it into two buckets, what technology am I using to protect my business, my employees, myself? And am I doing that in-house or am I working with a managed service provider? And no matter what, you gotta find the expert and it's worth the money.

is a key investment. that key, that strong piece around the right technology to make sure that you are secure. The second is the financial Protection and that's where cyber warranty such as that offered by Cork, cyber insurance offered by a wide variety of cyber insurance carriers, those are the financial promises that will be there if you potentially got hit. And so

many insurance brokers can help you on that journey, but of the million insurance brokers that exist in the United States, for

instance, very few of them are actually experts at cyber insurance in particular. That's why we focus on a few cyber insurance expert brokers.

One very successful partner of ours is called Datastream. Another is Fifthwall. There's a handful of these that are exceptional when it comes to taking care of modern business. ~ So those are those two elements. And when in doubt, call an expert, ask for

Martin Hinton (30:17)
Well, I want to move towards wrapping up.

Dan (30:19)
help.

Martin Hinton (30:19)
one of

the things I'd like to do at the end of all these is we've covered quite a bit of ground. Is there anything that you think we haven't covered that we should?

Dan (30:25)
The thing, it's a great question. And we live in a world where it seems like there's always a lot going on and there's the next drama ~ that's always about to happen and so many moving pieces and concerns and anxiety producing events. The thing that gives me great hope.

and excitement every day is that the vast majority of people that we get to interact with have love, kindness, spirit, drive, energy in their hearts, minds, and activity every day. And so I see that in my work. I see it in my own team. I see it in our industry. I see it on Main Street. And it is really exciting.

I believe that people come together in communities to support one another.

and we help share information. I see it all day long. And I'm really excited in just, I show up every day because I know that this world is a beautiful place to live in. And the threat actors that are out there, they can take some money, they can take some hits from, and they can cause some pain. But at the end of the day, we are a resilient race and we can show up and support one

And I love that about being human and embracing that human experience with one another.

Martin Hinton (31:58)
Well, I think that's a great note to end on. So first of all, Dan Candee

with Cork Protection. Thank you so very much for the time. It's been really, really interesting. To those of you watching, if you've got a question or a comment for me or for Dan, you can put it down in the comments section and we'll do our best to get the right answer to you. Also, if you enjoyed this, please share it. Please like it. Your support means everything to us. And with that, I'm Martin Hinton, the executive editor of Cyber Insurance News. Thank you for watching our latest podcast.

Enjoy the rest of your day.