0:01
Good morning. I'm Kevin O'Brien and this is the third in our coffee with series with the Mass Technology Leadership Council. I am the CEO and co-founder of Great Horn, a cloud based email

0:11
Security company, and I'm joined today by Deb Briggs, who is the chief security officer at Netscout.

0:18
As you can see, we're also working from home and Deb is joining us from her basement SOC Center.

0:24
Deb, obviously, is joining us from. The offices of Netscout. Deb, welcome.

0:28
Well, thank you, Kevin. Thanks for having me.

0:31
Yeah, it's a pleasure. So in this series, what we do is sit down for 3 to 5 minutes. You have quick conversations with security leaders in, and around doing that in Massachusetts area, really excited to have a conversation today around Ransomware. Deb, obviously news. But would you mind just sort of leave off and doing some orientation To where we sit today, as we think about what's going on in the rest of the world.

0:52
Yeah, so So Kevin, I mean it's, it's interesting on my way and I've picked up the Wall Street Journal and the headline today there wasn't something about ransomware but you know, we've seen more and more during this pandemic, that ransomware just continues to happen and it doesn't take a rocket scientist to know.

1:13
Why are people make money off of it. .

1:16
No, people continue to make money off of ransomware, it's going to continue to happen.

1:22
Yeah. No, I was reading the news this morning and seeing that there's this ongoing set of investigation, Superseding ransomware is now one of the attack tops that's being used by foreign nationals and for government against American companies. So there's this strong economic component to it, right? And so as we're recording this, Russia, just we think, took down the evil ransomware Bower crew. But obviously, changed a lot for many organizations with respect to the threat surface. What kinds of trends are you seeing?

1:55
Well, it's so a couple of things.

1:57
So as a CISO, You know, on a quarterly basis, I have to report up to the board.

2:04
I can tell you it's a board conversation.

2:07
Cybersecurity has been a board conversation for awhile, but boards are really interested in what you are doing about ransomware and how you are protecting yourself against it.

2:19
You know, some of those ransomware statistics that I just learned, too, when we were doing this, coffee with, with you, is the average downtime of ransomware is 21 days.

2:33
Were the then the average phase to total recovery.

2:37
It's almost 300 days since almost like a full year to completely recover, And when the board here statistics like this, they want to know what they're doing. In 20 20, you know, people who did ransomware They need $350 million.

2:53
I mean. why wouldn't they continue to do?

2:55
It's been really successful, and You know, if you're successful at doing something and raising millions of dollars, why wouldn't you continue to do it? So this trend is going to continue to increase.

3:07
You know, I think some of the statistics say that in 20 20 ransomware doubles, in 2021 is right on target for that. That same thing. So, you know, if you take Revel down, Someone else is going to pop up in their place.

3:21
and that's just what's happening. So is a CSIO or a security community?

3:26
We just, you know, we'd have to get better.

3:29
And, you know, it's, you know, you can be right and 99 times but that one time you're wrong. If it's ransomware, you know, it's a lot of sleepless nights to recover.

3:41
Yeah, I mean, I think we see that in all parts of the security framework right now.

3:45
Which is ransomware to credential theft, to phishing attacks, to sort of all of these different elements that she says, whom we work with are saying our board level conversation. And in part, the problem is become more difficult because we're all hybridized, working from home working remotely and now struggling to figure out what that attack surface looks like.

4:07
Often, when I talk to see says, what we're hearing is sort of looking for a defense in depth strategy approach to say it's not just one thing, it's not just the sharp line somewhere by having you know a piece of anti malware software, What's your take on that? Is there an element as defense in depth that we should be thinking about here?

4:24
So there's no silver bullet to ransomware because if there are we'd all be in that company would, you know, just be making millions of dollars.

4:33
I think no ransomware, You have to think of it is a series of steps, like you said, defense, event.

4:40
So if the ransomware event is boom.

4:44
If you think right of, boom, you've got three steps that you want to do, you want to identify what your assets are and what people know, where your data is, too. You want to protect what you have. And, Kevin, that's where you spoke about.

4:57
No? No, do you? How do you prevent phishing attacks? What are you doing to protect e-mail? Because e-mail is still one of the biggest attack vectors, even for ransomware, you know. And then the third step is you want to detect it once it's happening.

5:12
You know, some of the articles out there saying that when ransom, when they come in, when they get into your network, via a phishing campaign, or RDP or however, they, they get in fishing. Like I said, it's still the number one attack vector.

5:26
They're in there anywhere, weeks to three months before they.

5:30
No, they start encrypting everything. So they're learning what your network is there, you know, doing some burrowing tunneling within your network.

5:40
And I think, know, the defense, the defense in depth is protect. But I think we all need to figure out, when we look at the tech, what can we be doing? In our, there are a series of tools that we can do to me.

5:53
If someone's in your network, or anywhere, three weeks to three months, we do, then that's where we spend the majority of our time.

6:01
But I think with the headline, companies that are being ransomware, no, we can't walk the brain, which is once ranch and work, that you have to have a response of people to respond in the republic.

6:16
And I mean, it's huge.

6:18
No, I'm going to knock on wood.

6:21

No, I don't have any, I don't have any real life experience with ransomware nor do I want it, but, you know, we're working on right away right now.

6:31
So, you know, we have a ransomware playbook in a Recovery Book, and I know that type of an event happened is the C so someone responsible for security, there are a lot of things I need to do. The last thing that I want to be worried about is the recovery.

6:46
So, I've already partnered up with my operations team and the rest of the IT infrastructure team to say, Look, if we get hit with ransomware after the event, it's really a two prong event.

6:59
You know, I'm going to handle the cybersecurity piece in the containment and how did it get it, and, you know, shoring up that wall, but I need to focus my attention there.

7:09
I cannot be the person, the go to person, for recovery, so I think, is anybody involved in cybersecurity today?

7:16
You have to worry about, left of boom, but you can't just ignore, right? And you at least, have to have some sort of plan.

7:24
You know, I just think back to when my son was little, I think there's a Fire Safety Week in October, and we know they always say, you know, have a plan, if anything happens, how you're all going to get out of the house, and where you're all going to be.

7:39
I think we need to have at least that level of a plan for ransomware. You know, you always want to do left of boom and protected, but we all have to have a plan for, right? of, Boom. You have to have people, already, you know, knowing that, Hey, if this happens, you're going to all recovery.

7:57
And, hey, by the way, it how's recovery If it does happen, You know, 18 months ago, Kevin know We'd still be working in our home. So, you know, one of our disaster recovery is know your headquarters gets shut down due to a snowstorm or something. No one would have thought all our corporate offices were closed.

8:19
I mean, I think that sort of woke us all up for ransomware in the, Hey, if ransomware hits, um, know, this is going move fast. And you know, even if you catch it right away, there's still going to be days, weeks, months, worth of effort to recover. So you can't, you see, so can't be responsible for that recovery. So get that team lined up, and be partners in that, that team already.

8:47
Think those are really sage pieces of advice that it will probably leave our conversation at that. But I know that in the Mass Topology Leadership Council Committee, if she said, Is planning an event for in the early fall, I believe in Baltimore details on that to go into a discussion group, discussion amongst our members about ransomware. Because they're seeing

and strategies Yeah, thank you so much for taking the time with me this morning, and we'll speak soon.

9:10
All right. Thanks, guys. Stay safe.

9:13
Bye for now.