

you don't need to know everything that your machines are capable of right to have an incident response plan because adversaries are creative you're not trying to preempt every single possibility you're just trying to have process for the inevitable ones yeah and it really is like there's that story I I I've heard it multiple ways where you know somebody has a map and they wander through the jungle and they arrive at a city it's the wrong City but they they survive kind of thing even if you have a map that's wrong at least you're following a plan right and it's like do you have an incident response do you have a plan that you can follow that your team can follow because it can't also just be you Dre right like you being the the the the person we count on all the time who knows it all well what happens when you suddenly have to take your wife to the airport uh right after you give a webinar presentation like suddenly because I'm gonna say that your wife is not going to be very happy if she misses her flight I'm just guessing if somebody's like hey Dre we got this thing blowing up and you need to stop it you're you know well that's that's the part to burn out right and I mean this is the perfect example where sometimes there's about two people in an organization aren't following process and so in the incident on the screen you can see that we told a partner a handful of hours prior to a ransomware event like Hey we're seeing some early uh some early trade craft of an operation and because there wasn't any dialogue because there clearly was a missing process a missing response in the partner side it unfortunately did lead to to Ransom that's because there wasn't a response plan but the other thing is like improper instant response it's not just a cyber instance like it's a business continuity problem right like yes you need to be having a conversation with key decision makers if you're a service provider that's with your clients if you are in-house I.T that is going to be with those key Business Leaders and all of that gets you know it's business gotten new because what happens if there's a a flood a tornado um yes that wipes out all of your

computers right
have plans for that Ethan and that's
what's happening right and you speak to
people and I've spoken to people when I
did this response I'd be like you've got
a plan for all these other
inevabilities why don't you have a
cyber disaster plan right and what's
what's great about cyber disaster plan
or a procedure and process that's
written down is suddenly if it's a
client of yours
you've got something to give them you've
got something ahead of time that you
could say hey we're responsible and
you've got something when it inevitably
hits the fan that says hey we're not
Cowboys we know what we're doing here's
the plan that we're going to follow
doesn't have to be Iron tight like you
said Ethan amap is better than Nomad
it's about how you inspire confidence
around the people around you it's not
all
always about it being the most
technically accurate plan that could
ever exist