Th

So it would appear that one of the biggest vectors appears to be folk being sent email, the email containing an embedded link, then clicking on the link and then releasing all sorts of badness across the network that they're operating on. So unfortunately we all need email to operate in today's connected world, and it's very difficult to air gap or switch off email. So I think organizations need to look at manage [00:04:00] that, but don't actually stop the organization from actually working. I think aside from phishing emails, which is an interesting entry vector, my interest is what we call operational technology cybersecurity.

So the hardware and the software that controls things, and those things could be a myriad thing from street lighting within a municipality through to water treatment works. Unfortunately these systems are way behind the schedule when it [00:04:30] comes to cybersecurity and we've seen a number of attacks using OT systems as an entry point. There was a great example in a casino, admittedly not a municipality, but you could argue that a casino is a city in his own right and there was an attack there that came through the aquarium in the casino because the aquarium was the weak link and the bad folk got into the aquarium and they managed to move across the network. So I think the bottom because there are other safety systems in place, but if it had succeeded, then that water supply would've been poisoned and people drinking the water would've been impacted. So pretty serious danger there, Paul.

Paul Tis: Wow. [00:07:30] I can sympathize in terms of the electricity, just remembering just earlier this year we had some pretty significant weather events in Texas and we were just really not ready for it. So a lot of power outages and whatnot. Now, Rick and this question may be self-evident, but I am interested to dive into it nonetheless, but the question is, are smart cities, especially [00:08:00] vulnerable to cyber attacks, or are they better insulated from criminal behavior than other cities who may not have invested as much into their digital infrastructures?

Dr. Rick Robins...:

Dr. Rick Robins...: So I think in your previous comment, you identified one of those areas. It's not necessarily an eas around massive flooding or big fires or civil unrest [00:14:00] or something and certainly not cyber.

and the policies that follow for having a citywide digital agenda of which cyber should be an increasingly important part.

[00:30] how do the digital cspability linsocspe evol ing in that that se

Paul Tis: Then Nigel, my last question for today is how do you see municipal cybersecurity evolving over the next three to five years?

Nigel Stanley: I think the first thing is it's going to have to evolve, [00:17:30] Paul. I think that the local authorities have to understand that they are now very much in the cross hairs of the bad people that are looking to undertake cyber attacks and what have you. So no more is a municipality off limits and they will absolutely be part of the target. I think with budget constraints, I think that that poses a real challenge. So I think that the municipalities need to look at where they spend their money and how effectively they spend it. Unfortunately a cyber [00:18:00] event or an incident is a great way of releasing budget, but that's very much reactive, so what I would say is that they need to be looking at being proactive about managing the risk, because at the end of the day this is a risk to their business as it is for any organization.

timms.e that three to five years and how is that going to imhat

They need to factor that into their planning and in their budgetary spending. So it's going to be very interesting to see how all these various ransomware attacks carry on across local authorities, I think coupled with the massive budget constraints [00:18:30] that we're seeing within the public sector post COVID, I think is almost a perfect storm. So it's a real challenge, but no matter what these local authorities are going to have to improve their cybersecurity, whether they like to or not.

Paul Tis: Yeah, I think it's just going to be what we call table stakes, it's a cost to doing business and it's an unavoidable cost of doing business. Clearly the bad actors out there, both criminals as well as maybe [00:19:00] rogue states and rogue state agencies will not rest and will continue to look to exploit vulnerabilities. So there's a lot of good that can be done with smart cities and digital technology, but you have to be willing to protect your assets and your your citizens. So Rick, just kind of, as a add on to that question to Nigel cd o a 0ayber security evoliok,

cybersecurit?) TJETQ0.00000912 0.612 792 reW*nBT/F2 11 Tf1 0 0 1 2457 1 332.33 Tm0 g0 G[(TJE

lal justpberha tolseshof tling that I thinkpar going to eve ofro