This transcript was exported on Mar 15, 2022 - view latest version here.

Paul Tis: Well, thank you for listening to [Fwhen 00:00:15], I'm your host, [Paul Tis 00:00:16]. Today we're discussing cybersecurity with an emphasis on the built environment and the infrastructure needs of smart cities with Dr. Rick Robinson, Jacob's director of smart places, telecommunications and digital infrastructure [00:00:30] and Nigel Stanley Jacob's director of cybersecurity, People and Places Solutions. So Rick, Nigel, it's great to talk to both of you. Let me start with you Rick, get our discussion going with a question. How would you compare the level of malevolent cyber activity against municipalities versus against the private sector and or personal identity theft? How big a problem is this for cities?

Dr. Rick Robins...: So I think you can't really separate [00:01:00] cities from some of those other organizations, I've personally worked for an infrastructure company that along with many other companies in the British aisle and overseas was subject to a cyber attack several years ago, took out a lot of our systems for quite a long time. That therefore had an implication on our ability to keep infrastructures running. The company that I worked for, we reckoned that one in four of the UK population used something that we maintained or operated every day. So the potential footprint [00:01:30] there's already vast. There was a new story, not long ago, this year about a water company in America being attacked, so is it a city that's attacked or is it a company that operates an infrastructure for that city? These things are difficult to separate from each other.

I think what I would say is that the rate of deployment of digital technology in the built environment has been accelerating rapidly for many years now and will continue to do so from what was quite [00:02:00] a low base. As we deploy that technology and in particular, as we link data from one place of data from another or to an end user in another place or to a piece of infrastructure, all of those things having previously been separate from each other and hence perhaps hard to attack. As soon as we open them up a little bit to connect them to each other, we create vulnerabilities or at least the chance of vulnerabilities so that there is more to exploit. So I think this is already an issue, it's probably not one that we've spent [00:02:30] enough time looking to address, it's certainly one that will become a larger, more extensive issue with the potential for greater impact as we go forward.

Paul Tis: That's interesting. I suspect that with the advent of the COVID pandemic and those dispersed workforces and the need to really ramp up digital operations for companies that probably has even exacerbated the need for cybersecurity and [00:03:00] some of the potential opportunities for bad hat actors to do their dirty work. So Nigel what are some of the more common avenues of attack that hackers and cyber criminals seek to exploit when attacking municipalities. What are their main targets and what are their entry points?

Nigel Stanley: So that's a really great question, Paul. So we've seen a number of publicly acknowledged attacks across various municipalities in the UK and across the world [00:03:30] and almost inevitably it seems to come down to ransomware.

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 line is that the bad folk are increasingly creative [00:05:00] and looking for new ways of getting into these organizations and we are constantly on the back foot as we try and address this risk.

Paul Tis: That's interesting, I've heard anecdotal tales of cyber attacks occurring in things such as air conditioning systems and I think even vending machines, it's just anything to that's a connected device suddenly becomes a vulnerability or the potential for a vulnerability. So Nigel, can [00:05:30] you describe the dangers of cyber attacks against cities because outside of the financial ramifications, I suspect there are some public safety aspects that are worrisome like power grid, water quality, policing and that sort of thing. Can you talk to some of that?

Nigel Stanley: I think many of the dangers are self-evident. In the modern connected world that Rick and I work in, supporting the notion of a digital city where everything is connected [00:06:00] across a digital backbone, an interruption to that digital backbone could massively impact how that city operates, the first responders all the way through to the electricity supply. Electricity's fundamental to our day to day world and anyone that's ever endured any degree of a power outage would be very familiar with the visceral response you have to it because you realize that all the various gadgets, the world that you work [00:06:30] in stops working, which is quite stressful. I think an interesting stat that I heard a while back is that we are all three missed meals from anarchy.

In other words, if we end up missing three meals and it's completely an utter anarchy, which is a bit of a scary thought. As Rick mentioned, the attack on the Oldsmar water treatment works in Florida is fairly recent and then in that case, the bad people [00:07:00] got in there and they actually adjusted the levels of the sodium hydroxide chemical levels from the normal 100 parts per million to 11,000 parts per million. If that attack had succeeded, thankfully it didn't 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...: I think the answer to that question depends on how the smart city is implemented in each case. So a city that doesn't explicitly go down a smart city route, and I think high content actually, that's not really possible anymore, unless you as a city have somehow decided to rule out the use of technology. [00:08:30] Technology is getting baked into absolutely everything these days, so a city that doesn't look at that. Let's say perhaps deliberately doesn't create additional connections between infrastructures and control centers and swap data between different places, that city is avoiding, perhaps creating linkages between systems and data that could give rise to vulnerabilities that could be exploited or attacked. I think [00:09:00] linkages are nevertheless there, the infrastructures will have digital technology in the of various sorts that can be subject to attack, perhaps in the past that was less likely to happen because there weren't so many bad actors trying to exploit things or because it just hadn't come to their attention, there were more obvious targets, but I don't think you can rely on that being the case anymore.

Let's say a city takes a positive, smart city strategy and looks for delivering infrastructure that's got lower carbon emissions or greater consumer [00:09:30] convenience because it's using technology to operate intelligently or to offer a different way it can be accessed, then those steps will certainly create vulnerabilities or the risk of vulnerabilities. If it's done with a strong cyber strategy and a strong cyber governance, then you would hope that those risks are identified, they're mitigated, they're maintained, they're monitored, any threats and attacks are responded to and there you have a city that is in control of its cybersecurity. [00:10:00] If you undertake a positive smart city approach without considering the cybersecurity in that way, I would suggest you're taking rather a lot of very big risks.

Paul Tis: I can imagine that there's got to be more and more of a premium, I'm making sure you have a chief information security officer at the municipal level and if you don't have one, you need to find someone who operates in that capacity. So Rick, as a follow up to that, what [00:10:30] are the key areas of investment that municipalities need to focus on to ensure they are optimally protected from black hat behavior?

Dr. Rick Robins...: So I think in your previous comment, you identified one of those areas. It's not necessarily an easy area to address, so the city should certainly look at appointing a chief information security officer. The city isn't one thing, so if that CISO is appointed by the local authority, does he so [00:11:00] nevertheless have any oversight over the city's transport authority or water supplier or taxi drivers, or what shops do in the city. A city's ecosystem, it's community, it's economy are the aggregate effect of a huge number of disparate entities and so the task for a city CISO would be to create some form of governance over that ecosystem. Now that's not a simple thing to establish [00:11:30] and it would require a set of influencing policies as well as directive measures. So that's certainly something that a city should look to undertake.

I think then a key would be looking at what are the mechanisms that are in the remit of a local authority to influence what happens in the city? What criteria should be contained within any procurement policy for things that city procures directly. How could you use things like business rates frameworks or planning frameworks [00:12:00] to otherwise influence what happens within a city? A part of this is actually not going to be within local authority control or within any control within a city, some of it's going to be nationally regulated. If I think of the example of the UK's water and energy industries, for example, neither of those have a unit of governance at city level. The energy infrastructure is a national infrastructure upon which there is a competitive national [00:12:30] market of private sector providers, the franchise is to provide water are operated at regional level and both those sectors have a national regulatory body.

So that would be the root in for cyber governance through what are some incredibly important pieces of city operation and infrastructure. So it's a really complex area, but those are just some of the things that any authority should be looking at.

Paul Tis: Then Nigel, how would you describe municipal cyber defense in terms of the various departments cooperating [00:13:00] with each other? Meaning do you typically see police departments working with utilities such as water and electric, hospitals, et cetera, or do you see more of individual departments operating in silos?

Nigel Stanley: Great question. I think it's all of the above, quite frankly. I think it depends on the geography, it depends on the country where the municipality might be based in terms of the support they might or might not get. I think the one underlying constant is that all of these municipalities will be under [00:13:30] huge budget constraints and so if you look at an incident, you think, well, who's actually going to take the lead on that incident? Does it sit within the utility or is it a police problem or so on and so on. So I think that that's definitely going to be a challenge. Every single incident's going to be different. There are local resilience forums, I've done a lot of work, local resilience forums that bring together the first responder community but these groups are really focused around massive flooding or big fires or civil unrest [00:14:00] or something and certainly not cyber.

The question's got to be who would take the lead because every incident is going to be different, if it's a healthcare related cyber incident, is it the healthcare provider? Likewise, if it's criminal, is it the police and so on? We are assuming that these organizations such as the local Sheriff's department have got any expertise in cyber and certainly my experience is that many local and provincial police forces have very limited cyber expertise. So if they are looked to [00:14:30] take the lead, I think that they'll be maybe running away rather quickly. So it's a bit of a tough question really. I think an interesting model that we have in the UK, we have the national cybersecurity center and they were established a few years ago and they act as a useful coordinating body for major cybersecurity incidents, but they're unlikely to get involved with anything at the local municipal level as well. So I think that's going to be a bit of a challenge.

So I think the answer is unfortunately it [00:15:00] depends, but I would certainly suggest that local authorities look at how they deal with cyber, they need to accept that they will have a cyber event or that they will need to deal with and start practicing and rehearsal now with the various first responder communities to make sure that they respond appropriately.

Paul Tis: Rick are there any smart cities you would point to that are leading the way in terms of cyber defense maturity and capability?

Dr. Rick Robins...: That's a really [00:15:30] difficult question to answer actually because I think we're quite early in the emergence of the market. I think it has taken us a while to justify to business the importance of investing in cyber security properly, it's the sort of thing that at first glance doesn't appear to contribute towards the purpose of having a digital system. It of course has become increasingly about that, it's absolutely vital [00:16:00] to keeping that digital system operating the way that we need it to, but has tended to be the concern that's come second in the history of technology. We have certainly seen some interesting initiatives, so London for example, founded a digital security center many years ago, working with the police, local universities and the private sector supply side. So that's providing a resource, some capability and expertise in the sector, both [inaudible 00:16:28] and New York have accelerated programs [00:16:30] for cybersecurity startups.

There are several cities, ones I'm familiar with in the UK supporting the cyber industry would be Belfast and Dundee, for example, so there are lots of cities taking first steps. I think those perhaps in the strongest position to address this very complex area that we set out are those that have appointed at least a chief digital officer or chief technology officer, if perhaps not yet a chief information security officer. It's the sort of thing also that perhaps [00:17:00] a city resilience officer, such as Melan have had some time might play a role in. So at least if you see those roles in place, you see the leadership role and the start of governance and the policies that follow for having a citywide digital agenda of which cyber should be an increasingly important part.

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.

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 about cyber security evolution, , [00:19:30] how do the digital capability landscape evolving in that, that same timeframe, that three to five years, and how is that going to impact cybersecurity?

Dr. Rick Robins...: Well, just perhaps two examples of things that I think are going to, even from what we've seen through COVID continue to dramatically accelerate the deployment of technology in cities, one is climate change. So a lot of the infrastructure and asset investors that we talked at the moment think that three to five year timeframe [00:20:00] is the timeframe within which they have to act to make dramatic reductions to carbon in order to protect the 25 year asset value that they are interested in, that their business models depend on. They to act now to protect that asset value. Now, digital technology, isn't the only thing that we need to help us address climate change, but for sure using it to create infrastructure that is more efficient, more resilient, more sustainable, that's absolutely got to be a part of it. So we must see a significant deployment of [00:20:30] infrastructure using digital technology over the next few years.

The second one would be employment. The world economic forums future of jobs report in October last year predicted that between now and 2025, about 44% of the activities that form jobs today will be transformed by digital technology. That's an astonishingly rapid transformation. Another side to say, 44 percent of those things, a lot of that is going to be things that people do [00:21:00] in cities implying a lot more digital technology, supporting people who keep the buses running, who help us transport ourselves, who run shops, restaurants, all these normal things will continue to see a lot of digitalization. So we're going to see all of that accelerate and it will bring with it the need to be on the front foot and in control of the cybersecurity implications.

Paul Tis: Well, Rick and Nigel, I really appreciate you both spending the time to chat with me today about this topic. It's very fascinating and I [00:21:30] really appreciate your expertise. So thank you very much.

Nigel Stanley: Thank you, Paul.

Dr. Rick Robins...: Yeah. Thanks Paul.