ISSUE 48 | May/June 2021 | www.infrastructure-intelligence.com

INFRASTRUCTURE Intelligence

Why the future of infrastructure is digital

page 16-17

INDUSTRY BODIES

Hannah Vickers to leave ACE for new role with Mace.

page 6

FUNDING

What we know so far about the national infrastructure bank.

page 14-15

DIGITAL RISK

Don't be a honeypot for the cyber baddies.

page 22-23

Don't be a honeypot for the cyber baddies

Will the rush to smarter, digitally enabled solutions simply make life easier for cyber-criminals? *Nigel Stanley* assesses the risks and how to manage them.

Nigel Stanley is director of cybersecurity at Jacobs.

Read more online at www.infrastructure-intelligence.com

There is little doubt that infrastructure projects are seen as a way out of the current economic situation by many governments worldwide. We have all heard the UK government mantra of "Rebuilding Better" as millions of pounds are invested in new tunnels, railways, bridges and almost anything else you can think of.

But will this building frenzy create yet more opportunities for the cyber baddies to disrupt our way of life? Will the rush to smarter, digitally enabled solutions simply make the life of these bad actors even easier?

Almost every new infrastructure project is smart and digitally enabled. Sometimes this could be the sophisticated use of operational technology (OT) to control an entire railway network through to the more mundane building management system of a new office block or a road tunnel ventilation system. These new smart technologies are increasingly moving from proprietary serial-based networks to those using internet protocol control networks, often employing cheaper commercial off-the-shelf technology. In many cases, this technical infrastructure is identical to that in information technology (IT) networks used to provide email, file and print services.

And therein lies the rub. Where previously getting hold of hardware and software to replicate an OT network was costly and difficult, it is now a lot cheaper and easier. Internet auction sites are awash with anything from second-hand programmable logic controllers to industrial robots and production line equipment. Building a miniature digital city to hone hacking skills has never been cheaper. Similarly, the offensive cyber skills used by bad actors to disrupt our OT networks are increasingly similar to those they used for targeting IT networks.

All this opens up the world of infrastructure hacking to anyone with some spare cash, time and effort. The world of

cyber-attacks is like the fashion industry and infrastructure hacking is now suburban high street rather than haute couture. Bad actors can range from the archetypal lone enthusiast working away in a backroom through to sophisticated nation state funded groups intent on finding out how your latest water treatment plant works and what potential weak spots can be found.

The motivation can likewise be the fun of seeing a remote barrier move thousands of miles away, through to the more sinister grey zone cyberwarfare conducted by nation states preparing a range of actions ready to go when ordered by their political masters. Somewhere in between we have organised criminal groups who will see your infrastructure project as a tasty target for ransomware (where your data is locked away until you pay up) or blackmail. The latter being useful if you have a high-profile build such as a sports stadium that can be cyber-disrupted on match day.

A lot of the infrastructure we build will contain safety critical components that need to be protected, often according to a safety integrity level. These safety critical systems are now as vulnerable to the attention of bad actors as more mundane control systems. Whilst we find it difficult to understand why bad actors would want to subvert a safety system, they sure do. In Florida, USA, a water treatment plant was hacked in February 2021. This very nearly resulted in the levels of sodium hydroxide in the treated water rising by a factor of 100, potentially poisoning consumers. Thankfully in this incident other measures managed to prevent anything really nasty taking place.

Safety regulators and standards bodies have now woken up to this problem and are spreading the message that you can no longer be safe if you are not secure. Operators of essential services including electricity suppliers, water companies and those in the transportation and maritime sectors are now subject to increasing global oversight. In the UK, the network and information systems regulations carry a hefty penalty stick if supporting infrastructure and systems fail to address cyber-related issues.

So, what can you do to manage this cyber risk to your infrastructure project?

First you need to acknowledge that unfortunately your new project will be a honeypot for bad actors and your control systems will be explored by those with a bad motivation. OT cybersecurity risk needs to be 'designed into' every project you work on and right from the start. An experienced OT cybersecurity engineer can help conduct a risk assessment and identify weak spots in a design and likely routes an attacker can take. Conducted as an engineering lead process in the context of the business or project goal will optimise the effort required.

The other good news is that often very basic cybersecurity controls (such as changing default passwords, managing remote access, monitoring OT networks and educating appropriate personnel on their cybersecurity responsibilities) will make it much more difficult for your project to be subverted. Unfortunately, though, if a determined baddy wants to get into your project, they will, so having in place an up-to-date and well-rehearsed incident response and recovery plan will always pay dividends.

There are a lot of resources freely available in support of cyber securing infrastructure projects including those from the National Cyber Security Centre here in the UK and the US-based National Institute of Standards and Technology. Whatever your engineering discipline it would be worth taking a look at these websites and keeping up to date with the baddies - and what they could get up to around your new infrastructure honeypot.