TAKING CONTROL

Mike O'Malley *looks at the issues as Japan reveals a radical approach to securing IoT at a national level before the 2020 Olympics*

This time next year, all eyes will be turned towards Japan as we watch on in excited expectation as hundreds of sportsmen and women aim to achieve extraordinary things as they gather to celebrate the best of human endeavour. The 2020 Olympics and Paralympics in Japan will no doubt inspire and capture the imagination of every generation.

As such, Japan is acutely aware of the prestige and the magnitude of the event. So much so, that the Government passed an amendment to law, which will allow Government employees to hack into anyone's Internet of Things devices in a bid to secure the games and prevent any cyber disruptions.

Some 200 million devices – including cameras and routers – will be surveyed for password strength and Government officials will contact both the owners and

Picture credit: Getty

the ISPs (Internet Service Providers) if they're deemed high risk. It's expected they will find millions of devices operating with the default factory password settings.

It's radical. Yet, it's only radical because it is unprecedented. It is the first public announcement of its kind. It's the first time a government has declared it has the need to secure IoT on behalf of its citizens and the first time a government has actively recognised the threat of IoT to state security. It's justified. At the last winter Olympics numerous attacks were launched, but perhaps the most famous is the Olympic Destroyer launched by Russian state hackers dismayed at the decision to ban Russian athletes from competing.

RISE OF THE BOTS

This is against a backdrop of using millions of IoT devices to create botnets, now one of the biggest threats to cyber security we face. Bots can easily be recruited and organised into larger scale, high complexity attacks to interfere with broadcasting, utility infrastructure, emergency response communications and more.

It would seem then that taking such steps is a sound cyber security and PR strategy. No nation can afford to have the weight of a terrorist attack on its shoulders, especially during an international event. We're talking about major infrastructure outages, nuclear power stations being targeted, fibre and wireless networks going down and emergency services paralysed during the highest of high-profile events. Such is the state of cyber attacks today these events are no longer consigned to books of fiction. They are a very real and present danger.

Russia launched a cyber attack at the last Winter Olympics to highlight the fact that Russian athletes were banned from competing

WILL OTHER NATION STATES NEED TO ADOPT SIMILAR LEGISLATION TO JAPAN TO PROACTIVELY LIMIT THREATS?

If countries and companies are to invest in Japan, as so often happens after an Olympic event, and if Japan is to keep its position as a tech-savvy nation, then the measures it has taken are justified. Keep in mind, Tokyo had to out bid Istanbul and Madrid to win the 2020 games, and as reported in *The Washington Post*, it's expected to spend some $25 billion to showcase Japan as one of the elite nations in the world. This is high-stakes world diplomacy in action.

GOING TOO FAR?

Some people question whether they need to go to these lengths when it is not generally named as a nation that is readily targeted. And they have a point. However, sadly, as a host to countries that do attract cyber controversy, it's unavoidable. Russia, China, North Korea, Iran and Syria are all states that are often cited in cyber-security circles and their involvement is a red flag to a bull.

And as we know, the International Olympic Committee (IOC) is not immune either. It attracted a lot of attention from Anonymous during the Rio Games, keen to whip up a storm about social and geo-political injustice. It's inescapable that the Olympic platform is a way for insurgent rebels, political activists, or regular terrorists to pique the public's conscious or cause severe disruption and chaos.

In short, a high-profile event – be it the Olympics, the football World Cup, even the Super Bowl – has the ability to attract hackers of all walks of life and generate oceans of compromised IOT devices recruiting them to be enslaved into a massive botnet. But worst still, it can be used as a platform for terrorism. And while Japan's Government may have caused an outcry among its citizens for its apparent IOT activism, the hard, cold facts indicate it's an unavoidable measure.

In fact, as we look ahead to the 2024 Olympics or the 2022 World Cup, I expect France and Qatar will be considering a similar approach to protect its pride and trading aspirations, and keep the public – native and touring – safe, when they take their turn at hosting. But how have we reached such a situation that any government should have to step in and take matters into its own hands?

TAKING RESPONSIBILITY

The truth lies in the fact that no-one else has or will step in. If you ask security experts, companies making IoT services, and even the public who is responsible for IoT security they all say it's everyone else's problem. No one will take responsibility, and the best insurance policy for Japan is to take control and do all it can to mitigate the risk.

In fact, our research with senior executives shows that the ecosystem is equally split on security responsibility between the IOT device manufacturers, consumers/users, IOT application developers and service providers. And in this world, if everyone is responsible, no one is responsible.

Of course, there is nothing to suggest that people will take notice and the devices will be secured with a password change once they are identified as a risk or that an ISP will block all vulnerable devices. But isn't it better to get close to securing 80 percent or even half, than leaving the status quo we have today and securing none at all and simply hoping for the best?

Above all, it highlights it's an extremely complicated problem. And there is too much risk in relying on the industry to do something to address the problem itself and self-regulate the introduction of new IOT devices before next year.

With billions of devices out there, tens of thousands of IoT manufacturers and thousands of application makers it's an unwieldy ecosystem that no one person, government or NGO can get their arms around and truly own and manage. It's too big and too varied.

IDENTIFYING RISKS

Actively monitoring devices and identifying risks is the best option available, because let's face it to nationalise IoT is hugely unpalatable (at least for a democratic state). Instead, Japan can exercise some control and can pick up the threats well in advance and do something about it proactively to manage them. Their conscience is clear if they have taken all measures and means to close down threats.

I believe it signals a way for government collaboration the likes of which we've not seen before. Other nations may be moved to support the activity and help proactively and transparently manage IoT risk in their own countries during the Olympics, since with the internet, ultimately we are all connected.

▶

> THERE IS TOO MUCH RISK RELYING ON THE INDUSTRY TO DO SOMETHING TO ADDRESS THE PROBLEM

What's more, it highlights to service providers the risks and flaws they perpetuate. I can't think of anything more helpful than to have this government service if I were an enterprise that was trying to keep its own domain secure. Service providers have the domain knowledge and access to secure each businesses' devices and keep them secure. It's a gift to have a state co-ordinated effort – someone else rooting out the weak links and bearing the full expense of what can be a costly investigation.

Indeed, many security executives will hope that this prompts a debate on how IoT is secured in the future. And that we are moved to develop frameworks and best practice on how IoT applications are developed and secured from the moment the idea is conceived. Who knows, maybe this will prompt laws around the world that dictate IoT security. It seems a natural progression as we continue the evolution of a free and independent internet and put safeguards in place to limit hate speech, fake news and the unwanted spread of terrorist ideology.

SELF PROTECTION

Top of the list of issues to discuss is whether we can expect the IOT ecosystem to protect itself from infection and being co-opted into attacks. Will nation states need to adopt similar legislation to Japan to proactively limit threats?

I think in the short term we will see similar initiatives to Japan in democracies around the world. Especially in preparation for international events. Citizens will be encouraged to think about the implications through their legislatures and in particular, how proactive governments need to be. On the other hand, service providers will need to decide where and how they want to proactively offer IOT security services or be forced to do it through government mandate. There is much to debate, but Japan has opened the gates and without doubt that has to be a very good thing for us all ●

Mike O'Malley is the Vice President of Carrier Strategy for Radware, responsible for leading strategic initiatives for wireless, fixed and cloud service providers. Prior to Radware, Mike held various executive management positions leading growing business units at Tellabs, VASCO and Ericsson.

Though work has been underway to the physical infrastructure in Japan for sometime, a more radical approach is being adopted for the cyber realm

Picture credit: Getty