1 June 2017

Cyberthreat – a chilling new Pandemic

What was most frightening about the recent cyberattack affecting the NHS in the UK, was not the fact that it exposed how weak our national first responder network appeared in the face of a hostile attack (given some security experts were quoted in the media as saying the attack was not particularly sophisticated), but that the ransomware virus managed to scale 300,000 IT systems across an incredible 150 countries, shutting down critical telecommunications, utility and transportation infrastructures in under 48 hours.

Worse still, had the attack happened at the beginning of the week rather than at the end, the numbers could have been significantly worse. Regardless, it truly was the biggest global cyber offensive in history.

The fact that there was no direct loss of life as a result of the breach is more by chance than by design, so in many ways we have a lot to be thankful for. But the scale, and pace at which the WannaCry ransomware virus made a hostage of our most critical services across the world, means cyberterrorism has finally stepped out of the shadows and into the mainstream psyche of society. The world is finally waking up to the fact we are standing on a precipice.

Cyberterrorism has reached the point where tackling the threat is no longer just the responsibility of individual corporate businesses, or whole industries for that matter, it has perhaps even reached the point where the response transcends our police, our armed services and even our governments, but requires a collective response from joined up world organisations, to ensure every person in the world who owns a connected device is well educated and properly informed about the dangers within, and the precautions they need to take to be cyber-resilient.

Dr David Bray, Eisenhower Fellow and CIO of the US Federal Communications Commission, provides some stark insights to support this sentiment. He told the GSA "Some experts estimate there are approximately 20 billion network devices and 15 billion terabytes of data on the planet. The current trend is such that these numbers will double every two years, meaning by 2022, there will be between 75 billion and 300 billion network devices and 96 billion terabytes of digital content around the world.

With cyber-resiliency and the internet of things, maybe we need to approach it much more like public health than just building higher walls and tougher locks. What I mean by 'cyber' public health is yes, we teach you good hygiene, and we want you to practice good behaviours equivalent to seeing a 'cyber' doctor, getting the equivalent of security antibiotics and digital vaccinations etc. But we also recognise you still might get sick, and when you do get sick, it's really about rapid detection, rapidly addressing whatever the things are and then rapid clean up. We may need to think about the same thing for connected devices.

As an Eisenhower Fellow to Taiwan and Australia, I was asked by several private sector leaders "who is going to take care of your grandmother when her car gets hacked or when her refrigerator gets hacked?"

At least in my experience as a Fellow overseas, I'm not necessarily sure it's going to be law enforcement or even the military, I think it's going to have to be something new for cyber-resiliency and the internet of things, much like how we approach infectious disease and public health."

Technology has advanced exponentially since the birth of the world-wide-web, and arguably the human race is struggling to ensure there are the right checks and balances in place to adequately control it. If we don't find the right response, and on a global scale too, we might well find ourselves on the wrong side of the tipping point.

Until global leaders create a WHO-equivalent Task Force to combat the threat, private sector corporate organisations (and the trade bodies that represent them) must continue to shoulder the responsibility for educating their employees on the inherent dangers of being ever-connected to the Internet of Things. Most of the large and more established organisations have their own Information Security department (or equivalent), but there are many small and mid-size enterprises who don't, either because it's an overhead they can't afford or a risk they don't think is likely to occur. Either way, doing nothing is simply no longer an option!

The sourcing industry has of course been the pioneer of numerous innovations in tech and these days you can purchase pretty much anything-as-a-Service. Our industry boasts many specialist organisations who are proficient at monitoring cyberthreat, responding to attacks and providing information and education. These organisations can also deliver open-course and in-house training on cyber-related content ranging from general awareness right through to becoming a Certified Information Systems Security Professional.

UK firms suffer the highest number of cyber-attacks in Europe in any given week according to a recent poll, and are second only to the US globally when it comes to being targeted. What's more, the frequency of attacks is on the rise, with 16 per cent of UK firms experiencing a 10-20 per cent increase, versus 12 per cent overall.

The GSA is therefore reminding our members not to overlook the growing threat of cyber-attacks amidst the tsunamic push for digital enablement currently sweeping the sourcing industry. In launching the agenda for our UK Symposium we've acknowledged the increasing role that Digital, m-commerce, IoT, Automation and Big Data is playing in altering the sourcing paradigm, and how technology is changing the very ways in which the sourcing industry operates. We've also cautioned that the acceleration towards becoming digitally enabled must not be pursued at the expense of putting in place the proper safeguards against potential cyber threats.

To hear more about Cyberthreat, and the implications for everyone living in a hyper-connected world, hear Dr Bray in person at our annual GSA Symposium taking place on 27-28 June. **Click here** for more details and to register for the Symposium.

The GSA UK Symposium will take place on 27-28 June in Central London, featuring 11 programmes over 2 days focused on the growing digital aspect of the sourcing industry, future skills and location strategies, plus industry wide benchmarking results. Check out www.gsa-uk.com/gsa-symposium- 2017 for more details.

ENDS

About the GSA

The Global Sourcing Association (GSA) is the industry association and professional body for the global sourcing industry, and home of the Global Sourcing Standard. Its overriding objective is the ongoing development and dissemination of the Standard and supporting portfolio of qualifications to improve the benefits from, and positive reputation and therefore size of, the global sourcing industry. The GSA also serves to share best practice, trends and connections across the globe and to bring the global community together in a wholly interactive manner for the first time. The Global Sourcing Association UK, also known as GSA-UK, was formerly known as the National Outsourcing Association in the UK.

Media Enquiries - contact Tom Quigley/ Tel: 020 7292 8680 / Email: TomQ@gsa-uk.com.
Kerry Hallard, President of the Global Sourcing Association and CEO of the GSA UK, is available for interview – please contact Tom Quigley.