A New Frontier

By James Tate, Editor at sourcingfocus

Welcome to the wild west. The digital age is heralding a new frontier for the criminal classes. Sad to say it but, the sourcing industry and the wider society is woefully unprepared for a world of cyber-attacks affecting everything from cars to computers to fridges. A connected world offers so many opportunities for thieves, cyber-crime will be one of the major challenges of our generation. The GSA Symposium tackled the problem head on with a keynote presentation from two of the leading lights in cyber security, Dr David Bray, Eisenhower Fellow and Harvard Exec, alongside Donald Codling, Unit Chief at the FBI Cyber Division.

Before the Symposium, Dr Bray provided some comments on the growing cyber threat and how to improve cyber safety: *"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."

Data is becoming a huge draw for potential criminals as it can be copied, stored and used without the original owner ever knowing they were hacked. As we connect more applications and appliances to the internet of things (IoT), we increase the pool of data, creating more avenues and opportunities for cyber bandits to steal some digital loot. Recent attacks, such as WannaCry and Petya accessed systems through email, holding data to ransom and closing down airports, government departments, major global companies and Britain's National Health Service (NHS). As data becomes more important to the way we do business and live our lives, its value continues to grow. Major internet giants like Google, Apple and Amazon have built up huge stock market valuations as investors speculate on the potential future uses of the vaults of data that these companies hold.

We need to train people to look after their cyber health as many attacks, like with physical crime, rely on opportunities created by people being lazy. Teaching simple skills on cyber security can go a long way in reducing crime for a low amount of upfront investment. We need to be honest as to if we have been hacked as this can reduce opportunities for criminals in future as potential weaknesses are found and fixed. Finally, we need more accountability from major firms who deal in data and the digital world. The innovate first, fix later approach has inspired some of the great platforms and applications of the Silicon Valley age, but now we need to see more responsibility from the internet titans.

"EVERYTHING IS SPOILED. DON'T TELL ME IT'S NOT CYBERHACKING."

CartoonStock.com

Sadly, the fight against evil on the internet and in the digital economy is like Batman trying to clean up the mean streets of Gotham, it is a battle you cannot hope to win. Making the digital world safer is something we can do. A growing number of people are becoming aware of their data and are taking back control. The EU General Data Protection Regulation (GDPR) is encouraging firms to look after the security of all the data they have access to. The internet is here to stay, so all of that data will be accessible, try to make sure you know who is in control of it!

You can watch the GSA Symposium presentation here and learn more about cyber security.