CyberPro

April 5, 2012

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: JOHN SUFFOLK, HUAWEI TECHNOLOGIES LTD.

NSCI recently had the opportunity to interview John Suffolk, Huawei Technologies Ltd. John is a seasoned Global Business Executive having been a CIO three times; a Customer Services Director, an Operations Director and a Managing Director of a retail financial services organization accountable for £20bn of assets and a profit of £100m pa. He has run most business functions including IT, Customer Services, Sales (retail, telephone, internet), marketing, mergers and acquisitions (23 of them), and Directed/led many projects and programs up to £3bn in cost, 450,000 users with multi organization (70 different companies) with very complex delivery and stakeholder chains.

John recently retired from the UK Government after 7 years and did 5 years as Her Majesty's Government CIO and CISO, steering £16bn IT budget per annum using 50,000 IT professionals (after outsourcing). He is credited with driving the most dramatic change across the UK Public Sector since technology was first installed. He brought together central (Federal), regional and local government; delivering a citizen and business transformation agendas across the whole UK Public Sector of 5.5 million people and serving 60 million UK citizens.

His collaborative, open and transparent approach with a results driven focus has helped him win the best UK Company for customer excellence, his work has been a winner of the best retail financial services transformation program; and he has been IT innovator of the year. He has also been voted the most influential CIO by CBS and he has been ranked in the top 5 of the most influential people in technology behind Sir Tim Berners-Lee.

He is currently SVP and Global Cyber Security Officer at Huawei Technologies Ltd., a leading global information and communications technology (ICT) solutions provider that operates in 150 countries and serves a third of the planets population. He is also a technology and transformation adviser to the World Bank, helping growing countries transform public services.

In his spare time, he labors for his wife who runs a rare breed sheep farm in the Peak District in the United Kingdom.

NSCI: Can you tell us a little bit about Huawei and your key cyber security products and/or services?

Suffolk: I am not sure you can say a little about Huawei… First of all we are a global technology company that operates in 140 countries, where our technology supports a third of the planets population. We now employ 140,000 people (increased 20,000 in 2011 and will increase by a further 20,000 in 2012); We are used by 45 of the world's top 50 telecoms operators; we are a science and engineering based company with 7,500 PhD's, 50,000 R&D engineers and 50,000 patents to our name of which the majority are invention patents. We sit on around 130 standards boards in senior positions and are passionate about using standards to open up technology and communications to enrich people's lives. We have 26 R&D centers around the world and 23 joint innovation centers with some of

our key customers. We do everything from cloud computing to pipes (telecoms) and devices. We have products from AV and Firewall, to smart cities, to green data centers, and all things telecoms, education systems. I could go on for quite a long time.

NSCI: Any lessons learned you can provide regarding bringing together the various levels of government to work towards a common goal?

Suffolk: Well let us be brutally honest. Generally governments around the world are huge beasts and it can be painful enough bringing together one department never mind the fed, state and local elements. However what I can say is that Governments (as it is true with private companies) have a passion for getting it right for their citizens (or customers). So if you can come up with a compelling vision, a compelling story of what success looks like, and are not too prescriptive in terms of HOW you deliver, most people will follow that good common cause. If you insist that everything must be done your way, well, hell will freeze over first before you make progress.

NSCI: How would you describe the balance between transparency and privacy as it relates to personal information and cyber security?

Suffolk: A complete mess. At Huawei we have studied the law in just under 90 countries. What we find is there is much in common: privacy; data not to be captured and processed for purposes it was never intended; seeking consent from the citizen; good practice for ICT housekeeping etc. However the law is inconsistent – is IP address personal or not? In some countries the answer is yes, in others no. Can data leave country borders? Does local laws overrule international law; is the laws actually implemented: is there a common interpretation of the law? Well most of those answers are no. In relation to cyber security we are still at the "let's restate the problem" stage. I do not see much joined up positive action on addressing even the hygiene factors of cyber security.

But what we can see around the world is that there is a growing realization that as individuals we have become blasé about our own personal data and this has been coupled with the joining up and storing of data that goes beyond most people's wildest imagination. Law always follows reality by some years, and it is just awakening so we can expect significant pain, suffering and debate as we agree internationally (yes I am an optimist on some things) a more normalized approach to privacy and cyber security.

In terms of moving forward cyber security I think we still have another year of policy makers scratching their heads before we see concerted efforts to raise the quality and standards of cyber security (in its broadest sense) in Government and the private sector. It astounds me that Governments around the world are not mandated to undertake the basics of patching; whitelisting; reduced privileges etc.

NSCI: What do you think should, or could, be done to increase the "sphere of influence" of Security Officers within organizations?

Suffolk: Talk the language of the business. As a past CEO my day was driven by sales volume multiplied by margin minus my cost base – that was just to keep my head above water. Technology was a driver for my innovation and my differentiation. Security was only one issue that needed to be assessed. Unfortunately the posture of many security officers is one of defense – we all understand this – but as a CEO I wanted to know what I could do, not what I can't do. I wanted faith that my security teams would position me for being able to do more in the future rather than addressing yesterday's threat or at best today's threat. Of course the situation is much worse today but as a business executive I cannot lead the organization forward by looking in the rear view mirror – security has to be part of the solution.

So security teams need to work with their architects and sales and marketing experts to judge the likely product and service shape of the company in the forthcoming years. Security experts need to segment, "firewall" and limit contagion risk across technology – they must assess risk with reward and talk margin. Risk can be factored into price as is common in the financial services industry, so get the business to model and agree this approach. Risk is a board level debate so move the cyber risk into that area.

NSCI: Many have talked about a potential "Cyber Pearl Harbor," specifically as it relates to a major cyber attack on our critical infrastructure. How real would you say this kind of threat is?

Suffolk: I have pondered what would constitute a "cyber Pearl Harbor" and I would have thought we are well past that. We have probably lost more citizen and customer records than there are people on the planet; one gets the impression that there are more breaches of security than drops of rain; critical infrastructure has been breached; we have seen documentation showing that organizations are looking to invent in new malware that cannot be detected; what more do we need to say - we have a problem?

NSCI: What technology developments do you see as having the most bang-for-the-buck when it comes to improving cybersecurity?

Suffolk: I am a great believer in consistent, repeatable processes that gets the hygiene right every day but plans for the unknown and unexpected event. I am a great believer that we must invest in our employee's education – technology is generally not their core competence and nor is cyber security.

But I would say as ever and yes I know it is boring but:

- Patch third party applications and OS like a zealot
- Whitelist apps as best as you can – be ruthless
- Minimize admin privileges
- Install good IDS/IPS, Spam filters and the like
- Continuous exam based education for all of your employees
- Install employee monitoring software.

Now I know the last one raises the odd eyebrow around the world but the benefit I have seen of such software makes it worth its weight in gold. It can be difficult to spot the behavior of someone visiting strange sites to gather knowledge on how to breach your systems and steal your customer data!

NSCI: What do you think organizations should be doing to reduce the "insider threat"?

Suffolk: I have always believed that the culture of an organization is crucially important to the success of a business – not just on security – but on the whole company. I would always advise appropriate vetting of individuals, depending on their role, the appropriate use of electronic monitoring tools – which have saved the legal backside of more than one organization and can just stop people doing daft things. There is a balance to be struck between locking everything down which forces people to try and find ways around the controls or opening up the system and risking issues. Good employee monitoring across the entire infrastructure helps get that balance right. It is important that we continuously educate and inform every employee. It is also important that we factor security and the risk of the insider threat into the design and execution of our products and processes.

NSCI: What improvements are needed related to international response to cyber security issues?

Suffolk: Let's start with the basics and the toughest – the law. Any company that is international in nature and captures or processes citizen data internationally knows that data protection and personal privacy laws are a mess, inconsistent and in some instances unfathomable. Yet I saw a statement recently that suggested the reason why Europe doesn't have an equivalent Google or Facebook was because the privacy laws in European would reduce the profitability of the company by 50% so with profit as a proxy for the difference in privacy laws you get the measure of the differences. It is not just about privacy, we have seen the ongoing debate about what is acceptable behavior on the internet and the way different countries have different laws on "pam centers", computer misuse acts etc. We need as best as we can to drive to international standards on as much of this as we can.

Technology is the only industry in the world where you can turn off all of the safety facilities and the end user (in many countries) is not liable for their stupidity. I can be running equipment that is running the equivalent of the digital Black Death and jauntily spread my digital biological nastiness without a care in the world. Always cautious to step between the public and private sector in the debate about "what role ISP's" but we all have a role to play. How about we all internationally adopt the Australian DSD top 35 mitigation measures – OK let's not be greedy how about the top 5. How about Governments change the laws to make these measures mandatory, auditable and published by the auditors? Given that Government employees make up 20-25% of the global workforce in developed countries, how about they take their own medicine? How about we collectively set up validation labs to publicly prove the success rates of the anti virus/malware products. How would Joe Public know what he was buying was good or bad? Where are the international standards for the third party verification of critical software? Huawei puts its products through tough third party validation including providing access to the source code. Let's make this the standard.

If we change nothing, nothing will change, continuously pointing fingers is just diversion from our own inadequacies – we need to step up and start internationally working together – not conferences, not restating the problem, but doing real practical things.

NSCI: There are a lot of concerns regarding cloud security and bandwidth. How do you view these?

Suffolk: I am a passionate believer in cloud computing, but as with any new technology it brings new challenges. First of all for many unclassified systems, if you can satisfy yourself on the cloud provider, their skills in hygiene, you understand the local laws and users give their explicit consent to their data being stored (somewhere – and they do need to know), then go for it. Will we see data loss, yes, but we see this today and at least we can use our scarce resource to fix cloud environments rather than tens of thousands of small ICT estates.

For classified material the cloud still works but clearly at the edge Governments will wish to add their own propriety tools and techniques to reduce leakage.

But researchers around the world again need to come together to think through the new challenges. Huawei has a cloud security research team in Beijing and we are looking at new models and we would be delighted to share our thinking with anyone who wishes to collaborate.

NSCI: Is there anything else you'd like to add?

Suffolk: Having done big banking roles, run my own consultancy, transformed the UK criminal justice sector and been the UK Government CIO and CISO for 5 years, cyber is the thing that will reduce the adoption of technology globally. If, like me, you believe that technology enriches people's lives then collectively we must work together. At Huawei we will work with any standards body, any researchers, any CIO's/CISO's and Governments to address this issue. We look forward to working with you.

NSCI: Thank you very much for taking the time to visit with us.