APPG ON CYBER SECURITY MEETING AGENDA 25th May 2022

Title: The meeting will hear from three experts in cyber security / Local Government about the challenges faced by our Councils and how these are being dealt with at a local level.

Chairman's welcome – thanked and introduced the speakers.
Apologies: Admiral Lord West
Speakers:

1) Dr Andrew Larner, Chief Executive, iESE

iESE – local Government owned and created business. Offers a shared resource to help Councils modernize what they do: leading edge best practices, practical consultancy; digital arm.

Not coping as well as we should with cyber threats and a digital future will only expand the angles of attack into the infrastructure. A number of Councils are building IOTs for instance to stimulate growth. Not sure that all are coping with where they are now. Produced a paper based on an audit of five Councils. Resources and knowledge are hard to come by in cyber.

Local Govt is good at sharing learning and best practice. Councils have experience with the current generation of cyber security tools but the problem is in the increasing sophistication of attack. Attacks are more sophisticated and some involve overseas actors. IESE has expertise in procurement and only found one tool to use which was successful. But this is a problem, a single product in the market makes it difficult to push in Government circles.

Need to learn from when things go wrong. More than 12 Councils in the last 2 years have had expensive and significant failures. Hackney has still not got access to their social care records a year after being hacked as an example. This is a big warning sign.

Seek to share "worst" practices and learn the lesson of those incidents in an environment in which sharing this type of information is not the natural thing to do. LGA more likely to say that one cannot talk about a given incident. Need to be more open about what has gone wrong.

2) David Woodfine, CISSP, Managing Director, Cyber Security Associates

Based in Gloucestershire which is becoming a centre of cyber security in the UK. Ex-military (RAF), attacked by Conficker[1] virus in 2007 -08 and some of the IT estate was very vulnerable to this virus. Some RAF bases lost significant capability. The concern that came out of this was business IT vs operational technology.

[1] Conficker - Wikipedia

RAF Coningsby was running a platform to support Typhoons which were plugged into both operational networks (to tell base how the plane was operating) and secret networks for programming missions. Threat that the virus could move from operational to business systems. Attack was aimed at the MOD Supply Chain.

Contractor did not know how to deal with it and the aim of the attack was clearly to get into the contractor system. Allowed the MOD to invest more in cyber security.

DW also conducted offensive cyber operations and left in 2013 to set up Cyber Security Associates to look at how we face a cyber threat together. Nowadays there is more data available so the threat landscape has increased significantly. Criminals, whether State actors or not, have more resource to put into a cyber attack.

Have to keep our Critical National Infrastructure working and this is where cyber attackers will try to enter the system. Works with clients to provide a defence in depth. Cyber security starts with people then technology. Everyone needs to know how to respond to a data breach and an attack. Organisations are realising that they cannot ignore threats and need to invest in their cyber security posture.

Russia / Ukraine – Russian capabilities seem to be more focused on Ukraine and not attacking the West. NCSC are a great resource and have indicated that the UK must remain at a heightened state of alert. Not only threatened by Russians but other state actors such as China and North Korea.

3) David Cowan, **Head of ICT,** Copeland Borough Council

DC was the first PSN technical director and have worked for multiple local authorities. Came to Copeland by request from a major UK bank. Copeland was suffering a major attack and needed help. Typical small English District Council with 320 staff. Home to the UK's largest nuclear sites but also the first UK Council to have suffered a major attack which took all systems offline for 6 months.

Took 2 years to recover from this attack. All Councils are under financial pressure and Copeland[2] lost £2.5m in terms of cash out of the door when compared to an annual expenditure of £9m. Redcar[3] lost £10m thanks to an attack. For less money all Councils could be protected. Work to help other Councils learn the lessons.

[2] Council hit by cyber attack reveals £2m cost - BBC News
[3] Redcar cyber-attack 'cost council £10.4m' - BBC News

Every day sees multiple examples of attacks against the organisation and individuals. Have defences in place to log, capture and stop. Only takes one attacker to get through and they have won. Sees an increase in volume of attacks.

General level of preparedness is not where it needs to be. Smarter about collaboration across the sector. Biggest worry are the silent and disengaged Councils, some are sleepwalking into a major issue, only wake up when the attack happens.

Copeland lost its Land Charges records which effects all those buying and selling property in the area. From a skilling point of view not easy, in banking DC had a 70 seat SOC and paid the money to fill the seats, although only had 50% full. In a small Council in the NW, hard to recruit people. Works closely with the local nuclear sector who have the same recruitment problem. Wants to share and gets frustrated when agencies tell Councils not to share, good to share information.

LGA doing great work, Cabinet Office, NCSC, Dept for Levelling Up also contribute well. Pan-Government Assurance was an aim of the PSN, we do not have a pan-Government Cyber Policy and this exacerbates the situation. Councils tend to look to central Government and have to comply with multiple regimes. Just wants one across the whole of the UK Government.

Open questions and discussion –
SF – understood that threats, typology etc. were shared by NCSC. What do you want to see?
AL – not just what but the timeliness of sharing information. Used to run a number of networks in Local Govt, when something happened it was out within minutes. People were minded to help each other, going back some time.

There used to be the Beacons scheme in Local Govt and there was more emphasis at Cabinet level in terms of sending staff to keep up their knowledge. This included managers as well as specialists.

Tim Rawlins – why is there a reluctance in Councils to take up free resource. NCC was commissioned to offer this and sometime Councils resisted the offer of free education. What is the key reason for this? This was from the Cabinet Office to Chief Executives in Councils.

AL - when we run a campaign we get in excess of 96% penetration. Would need to know who you were targeting, details etc. Maybe it was a language issue or internal communications.

DC – numerous reasons. Targeting is crucial, you need to put a message out jointly across different central Govt departments. Typically get inundated with supplier messages, so the message must come from Govt or the LGA / iESE.

Free help costs us resource which we may not have so that is another reason that it is hard for Councils to engage.

Steve Pass – focused on the growth of Smart Cities which will increase the attack surface. Local Authorities need to expand their abilities to defend themselves.

SF – look at Smart Cities as a specific topic.

Sofie Dralle – interested in the point on certificates when hiring people. How do you upskill people as part of their job and to increase the pool of candidates for hiring.

DC – certifications I referred to are CISSP and CISM which are available in the UK. Not entry level, require 5 years' experience to apply for the qualification. Many others as well, it is not a closed marketplace. You need CISSP and CISM to work for the US Govt.

DW – need to look at certs for organisations: Cyber Essentials and ISO 27001. I am a CISSP member and need to encourage youngster to look at Cyber Security at a secondary level. Very encouraged by an apprenticeship scheme, cyber bootcamps etc. Up to companies to invest in their people and get them onto the first rung of the ladder.

Malcom Warr – set up business resilience centre network also have nuclear experience. Why can't we get together through the business resilience networks to share experiences.

DW – part of Gloucester First LEP cyber partnership, my role is to pass information on from this group to businesses in Gloucestershire. Getting better and need to replicate this more widely.

AL – local models are great, proposal is sensible

DC – what already exists in Local Govt is the WARP network which also covers Bluelight. Meets regularly and members are all typically Councils, NHS, Police so there is some cross over. Constant discussion about how much it should include local business.

MW – should be taken up by Central Govt. Clearly a problem that we are not communicating and there are lots of gaps. Should pursue through Parliament.

Baroness Uddin – have a local Govt background. Very alarmed to learn about data loss and the implications of this. A National Strategy is essential, Central Govt is able to dictate strategy and directions which bind local Authorities.

Apprenticeships are clearly dominated by the “usual suspects”, how do we bring in the unemployed, those who are educated but not interested in this area?

Prof Keith Mayes – observation: you have these different agencies putting forward different security policies which is a waste of money and leads to contradictions and loopholes. I would recommend that the APPG tries to escalate this and ask what are you doing to harmonise this?

Secondly, one has a number of local Authorities and the suggestion that they build their own practices. Is there a strategy for local Councils to get together to have a pooled service which is shared?

AL – both! iESE has created the capacity to serve the sector and growing that. The people involved in this are very experienced and individual Councils could not hire people at this level. Trying to roll this out across the sector.

SF – will take it this to Steve Barclay.

Graham Mann – smart Cities and Digital Transformation is a key area to look at. One of the issues raised by Dave is the advanced attacks and the difficulty of recruiting good people. Keith’s comment is at the nub of my question. Why can we not have a centralized SOC for Councils to provide best in class capability?

AL – iESE has adopted that capability as members have asked for this so some Councils are involved. Have used a collaborative approach with Councils before to get them working together, digitization of the Ordnance Survey map base is an example.

DW – important that we defend UK plc, cannot have 220+ different SOCs supporting different models.

Steve Pass – what more can we do as a collective? There are many parts in defending Councils centrally and efficiently such as a Fire Gap back up done on a central basis. How can some of the private companies be more supportive as well?

DC – NCSC is looking to commission such a back-up service for Councils. Interest in sector wide SOCs, there are discussion going on with the agencies.

Conclusions – Shows the scale of the challenge, will raise with relevant Ministers.

Next meeting – 4th July on Cyber Security and Humanitarian Aid