APPG ON CYBER SECURITY MEETING ON CYBER SECURITY & THE DIGITAL DIVIDE - 5TH DECEMBER 2022

Title: The purpose of the meeting is to look at how the Cyber Security world is trying to bridge the digital divide. How do we help people become and stay security aware when many find it difficult for a multiplicity of reasons?

Chairman's welcome
Apologies: Baroness Neville-Jones, Lord Taylor of Warwick
Speakers:

1) Jon France

Information Security professional and CISO at (ISC)2 serving as advocate for security and risk management activities, skills development and awareness amongst all users of technology.

There are 4 areas to look at:

i. Age
ii. Skilling
iii. Socio-economic factors
iv. Access to technology.

Take 5 campaign was an excellent way to raise the issue of fraud in the financial world with the general population.

Issue does worry me. ISC2 has an annual workforce study, from last year's one, it was found that the UK needs an extra 56,000 cyber security professionals. Most companies do not have a member of staff who looks after cyber security for more than 20% of their time. Need to drive up recognition of this in the corporate world.

Education is important for improving baseline knowledge from an early age. It will help to future proof the country. Digital natives need to help the digital naive.

Economically, you get the best deals online so if you are not a cyber native, you lose out. The least advantaged in the country do not have access to the best deals. Google have opened a research centre to design technology for the less-abled. Takes heart from this.

2) Ian Jenkins (see attached slides)

Ian is a highly capable, experienced, information protection and risk professional, with a track record of delivering successful and complex change programmes across major enterprises. He works for the Cyber Leaders Network helping people at the CSuite level better understand Cyber Security. Recently spent time with Age UK. Pragmatically, how do we get people online who are not there and how do we get people to be cyber secure?

ONS by 2025 1 in 6 will be 65 years+
Vodafone and Gloria Hunniford worked together on the Hi Digital platform aimed at senior citizens. They found out that 45% of over 65s are not comfortable going online. Moreover, those in later life could lose £1000 annually through not accessing offers and deals. 38% feel forgotten when digital first is the default. 34% feel stressed going online. For those online 41% did not know where to go for help. 27% who are comfortable online would benefit from learning new skills. Half of those surveyed cited security and scams as a major deterrent from using online services.

Companies or Govt departments have to offer expensive exceptions management process for the digitally excluded and struggle to do so. Could this cost be significantly reduced with more online?

The 3rd sector generally lags behind in information protection and cyber security and is a known soft target for hackers and scammers.

Could UK digital suppliers supply a simple booklet at the point of sale to give guidance?
Could Online sources of help be made more readily available through apps and online services?
Better publicise the financial and practical benefits about being online. There is a lot of noise about ransomware attacks, scams etc. that frightens people.

Consider regulation for the 3rd sector – make the transition to best practice more 'push' than pull. Only 50% are aware of the consequences of a cyber attack. (See slides for other figures). Charities are passionate about delivering services to their clients but cyber security is rarely a Board level matter. Charities do handle large amounts of personal data on behalf of citizens. Some charities have long supply chains which involve partners who are large and others which are very small. The supply chain relies on a number of players with various levels of cyber awareness and security, all contributing to risk.

The digital divide is surprising when compared by regions across the UK as the figures show.

3) Dr Emma Philpott MBE:

Emma is CEO of the IASME Consortium Ltd, an organisation that delivers accessible cyber security certification for smaller organisations and supply chains. Emma is also Founder and Manager of the UK Cyber Security Forum, a not-for-profit organisation leading an initiative to train unemployed neuro-diverse adults in cyber security and supporting them to find employment. In 2019 Emma was awarded an MBE for services to cyber security.

Cyber Essentials partner for the NCSC. Train up neuro-diverse adults in Hereford and Worcestershire. Do end up employing many of these people at IASME. Understands the benefit of supporting neuro-diverse employees. 40% of the staff are neuro-diverse.

Almost 50% of the organisation is female. Certify 2000 organisations pcm through Cyber Essentials. Keep coming up against the digital divide with the elderly, those with learning difficulties etc. This problem has been in place for a long time. There is a lot of advice and guidance for the elderly but it is not working as we see fraud rising. 80% of fraud in 2021 was through a digital device, the highest losses are in the older age groups. Furthermore fraud has an effect on mental and physical health.

Important to protect people when they go online. If you are hit by fraud online once, you are likely to be attacked a second time as criminals share lists. Cyber criminals particularly target older people.

For those who are not digital natives, going online can be confusing. IASME has a proposed solution working with Housing Associations or Old People's homes offering devices that enables the basic technical controls. Will also secure social media accounts with passwords and privacy settings. This will be done on a face-to-face basis. Devices will be monitored to prevent people from accessing known scammers' addresses. Will start a pilot in the next few weeks. Will start with 50 people and see what happens.

Open questions and discussion –

Simon Fell MP – Prior to the Take 5 campaign we had a "beware what you share" one. What should the next campaign be to address that gap?
JF – should not be online!
IJ – Where are the places I should go, what are the channels: Citizens Advice, International Age etc. Reassurance that online can be a positive experience. Very tricky as any guidance must be easily understood and jargon free.
EP – campaigns are great but what about aiming at the families to look after their granny?

Pat Keane – part of a group Volunteers Against Scams. Groups seem to be missing the point about reaching their audience.
EP – Too easy to click on the wrong link and trying to explain what to do is difficult
JF – where is the help when you have been pawned? How do we overcome fear and embarrassment?
SF – Banks are good at supporting their customers when they have been scammed if you tell them up front.
IJ – Tech providers – are they as proactive with individuals in the way they are with other companies? Should there be a duty of care?

Lesley Charteris – Could youth organisations like the Boy Scouts have a badge for teaching cyber security / hygiene? Capita run sessions for staff and families.
JF – the age problem will work itself out over the next decade or so as we who are cyber experienced grow older.
IJ – whatever we do needs to be scalable. The overall numbers are significant. The pace at which computing and threats change is exponential so we will find that these threats becoming more challenging.
EP – who is in a trusted position to advise on cyber security? Someone who is insured, covered by DBS and employed. Need to be careful about the people you use to do the teaching!
SF – need to be aware of the barriers such as difficulty recalling passwords.

Mike Hurst – cited the difficulties of aging e.g. failing eyesight or mental health issues which make accessing online services impossible. Talked about hospitals not sending out letters as this is no longer an option. As cognitive ability goes down, systems need to take this and physical disability into account. Need to understand the requirements of the end user.
IJ – one of the problems that you describe represents the exceptions management cost. Need to understand the end-user needs and at scale, and see what can be achieved Vs cost/savings

Lisa Addison - Chelsea Hospital has 300k patients per year and it is impossible to go completely paperless. My father cannot look at this phone for his hospital appointments.
SF – fascinated to talk to an Internet SP about stopping people who are undergoing a manic episode from buying goods and services online during that episode. Online is a problem for those with dementia or losing faculties.
IJ – Age UK wants to be engaged with the topic as it embraces those in later life and to help develop thinking.

Neil Sinclair – 1) key thing is where people go to get help. Person in the street has no idea where to go for help. NCSC is the go-to point but cyber looks complicated etc.
2) Number of companies who do training once and never do it again! We learn in different ways: printed word, pictures.
3) Needs to be cultural, like the IASME Highway Code.
JF – looking at how to get people involved in cyber security. In the NHS we have to design security in with low friction. This is a particularly bad example of bad design.
PK – not beyond MS to put in a little warning when people click on a link just asking them to think about what they are doing.
LC – What about the nudge theory? It all costs money which is the problem. The Govt has just issued new advice for schools but not mandated that advice which would mean spending money. Teachers get basic training but do not share it with their pupils.
EP – very easy to say MS should do it or the Govt should fund it. What IASME are trying to do is to say what can we do now? Providing devices is not what IASME does but is willing to try issuing these devices to see what might happen. Funding it themselves as IASME could not find anyone to fund it at a cost of £26000. How can we take a step forward? We will only stop a bit of it.
Talking to Housing Associations about funding this long term. Police will give advice on security in the home to prevent burglary but not cyber crime.
LA – Responsibility is at the Governmental / National level.
IJ – strategic providers have a duty of care, often have CSR programmes that could help fund initiatives such as Vodafone's 'Hi Digital' offering with international Age.

Gerard Phillips - Cyber helpline is a great resource.
My experience is that people are intelligent and self-reliant. Ran course in Brighton for older people and found that if you give people the basic information they will take the initiative. 88 year old father in law is an online investor. It is a complex business.
IJ – Need to remember the truly 'digitally excluded' - if you earn less than £10k you are less likely to be online – perhaps opportunity cost from seeing more online also offers potential to help release spend for provisioning.
JF – there is an economic divide.

Mike Hurst – telcos want to sell connectivity and therefore laptops, could the IASME device be included.
Neil – found that cost implications and staff training were key blockers as well as liability.
PK – perception is that there is no money in providing cyber security services to older people.
JF – MS have put a lot of effort into securing their platform but not around fraud or users.
SF – pre being an MP tried to get financial fraud included as a topic in schools but DfE not supportive due to a lack of teaching time.
Sanjana – runs a charity for face to face with young professional coaching children. Younger people's attitude towards social media is very different. Huge variance in knowledge amongst senior citizens. Making senior citizens reliant on grandchildren is the worst thing as you are not educating them. Some of my young professionals have not heard of the apps which young people use. Parents need to teach their children from the start. Begins at home!

Conclusions -

SF – if you had fireworks in the home you would be very careful. Thanked the speakers and the audience.