N8 Policing Research Partnership: Innovation Forum on Cybercrime

Market Place Discussions

4. Stakeholders, Business Engagement

The Research Idea	Empower vulnerable SMEs to protect themselves from cyber crime - Understand who is vulnerable - Barriers and incentives faced in addressing cybercrime
Stakeholders	SMEs, crime prevention teams, academics, financial service providers, "SME growth" infrastructure, Federation of Small Businesses
Resources Required	Research time to scope out what is already known Action learning set and facilitators
Funding Sources	H2020 NESTA? Home Office?
Key contacts from Innovation Forum	Sarah Williams – WYP Paul Wainwright – Humberside Police Matt Walker – NY Police Ann Pittard – Keele University Cheryl Simnell-Binning – Lancaster University Nicky William
Next Steps/Who will do What and When?	Scoping existing knowledge Connect to vulnerable groups/victims/forum group to understand impact/profile of SMEs affected Facilitate and review action learning sets

Notes:

- How to **empower** vulnerable (vulnerable as in victims or through own error) communities to protect themselves
- Which stakeholders/supporters of SMEs and capable to advise SMEs in the N8 region
- What is an appropriate offer
- Who are the vulnerable SMEs
    - Which groups of business/types of business
    - Urban/rural
    - What drives vulnerability – policing, technology
- What are the barriers/incentives to SMEs engaging in cyber essentials – eg costs, knowledge, culture/language, trust, training
- Scope for mentorships, advice and guidance on cybercrime – action learning
- What works in
    - driving awareness/action: leadership in government/ business/ city/ police/ governance
    - in supporting change in behaviour
    - solutions, stored services
- Implications for HR practice
- Stakeholders

    - Larger organisations – supply chain/CSR on IT requirements
    - Business organisations - chambers/trade bodies/TS advice and infrastructure bodies
    - Third sector
    - Public sector
    - Financial services sector – banks, accountants
    - "SME growth" infrastructure – Santander, GSF, £10k
    - PCCs – as champions
    - Police – crime reduction teams
- Learn from others, eg Manchester Information Security Group for large organisations
- Cyber security information partnership
- Health – self-managed patents
- AQL
- How do SMEs access information/learn
- Funders: NESTA (open innovation), LEP, Home office, H2020
- Next steps
    - Scoping: what's out there? (academic, grey literature, current 'policing', business community, FSB data, cyber essentials, national threats applicable to SMEs)
    - Barriers
    - Vulnerable groups: nature of harm to SMEs, connect to other groups
    - Action learning set(s): issue, learn/change, review

Rapporteur Notes:

Attendees:

Jo Cutter (1), Sarah Williams – Police (2), Ceri Virtue – Police (3), Cheryl Simmill-Binning - Lancaster Uni (4), Ann Pittard - Keele University (5), Nikki Williams (6), Matt Walker (7), Paul Wainright (8)

Jo – What sparked interest in this group?

Sarah – Collaboration – how much do the police know? Banking, other agencies involved – police can't deal with it by ourselves.

Matt – About privacy. Whatever type of crime has cyber element, public expectation police will deal with it because defined as a 'crime' – but type of crime where many stakeholders must be involved. Can work with others to retain data and share data – is there anything with can use as a leverage to get them involved? Can we legislate this?

Paul – Interest on business side. Talk about impact on small and medium businesses, can we help them? Can we work with them? Chorale them together? Not many SMEs have insurance to cover themselves. Need focus on smaller business community.

Ceri – Where do SMEs go for good advice? Start-up or growth businesses looking for trusted source. Police might not be interested in them and they couldn't approach them. Who else do you go to?

Paul – Cites example of a virtual network – tells company what's coming. Smaller businesses might not be able to see relevance to these networks.

Nikki – Information partnerships, what police are trying to do – she teaches computer science. Wants students to have awareness, know when should call in police – interested in training. Why scenarios interest one individual and not another – tailor this to training so they know what works for them.

Ann – Specialist students could go into specific areas. Computer science departments in universities could be of use.

Sarah – People don't understand they're victims of cybercrime. Some vulnerable groups we protect better – eg. 8 year old, 65 year old. How do we look at different levels of vulnerability and educate people as to how they can protect themselves?

Jo – Who are the victims?

Sarah – How do you engage with the education component of that?

Jo – Emphasis on businesses without forgetting there are other groups.

Paul – How do we define communities?

Cheryl – Something there – we are all being forced to use IT. May not want to use it.

Jo – May need to understand the drivers of vulnerability. Cheryl asking how does public policy in other areas create vulnerabilities?

Paul – Example about plumber using app to take money, not cash, and money stolen. Could snowball on large scale.

Ann – Larger businesses might be focused on protecting their business – where are the gaps? Can you include these companies or is this something they might closely guard?

Matt – Loyalties of bigger businesses may be to shareholders, and customers come second. They don't want to tell police when something has happened – may try to deal with it in house. But data could be shared. This is a big challenge.

Jo – Institute for Data analytics at Leeds trying to tackle this problem. About data that comes in and extent to which people are willing to combine and share data. Sometimes businesses collect huge amount of data, but don't share. How do you develop approaches to analyse this data in a way that there isn't a direct product company can sell? How do you make it available? Store Club cards, phone records, being examined in terms of open data. Strand fo NPaul(ph) program around data analytics.

Ann – Different ways of creating change.

Jo – How do you balance diverse interests of different sets of organisations and institutions? Can't just ask companies for their data. May be able to compel them through legislation or their shareholders – interesting dimensions to explore.

Cheryl – The more NHS becomes private, they have different interfaces. You think you're giving information to NHS but goes to other agencies. Eg. pharmacy prescribing prescription only drugs – access to patient's confidential info. It is being handled carefully. Issue is not problem she's working on but when they replicate it in the future and may not adhere to same standards.

Paul – Beyond chemists.

Jo – Two core areas – 1) SME community and 2) what's driving vulnerabilities around different groups. Task is to summarise data in sheets.

Headings of sheet: Research idea, stakeholders, resources required, funding sources, key contacts from innovation forum, next steps/who will do what?

What is key research idea or question?

Matt – Key areas of sustainability of communities is economic infrastructure. Need to make communities attractive place to operate. What stakeholders can be involved in giving businesses who want to run in areas opportunity? How do we keep people in the community? If people going to London because better support networks, will lose business in North. Which stakeholders/ supporters of SMEs are capable/able to advise on CC in the NS region?

Paul – Need to pick out most vulnerable and focus on them. We can't do everything. Picking out some and focusing. If you do that others might want to know what's happening.

Nikki – Why some of SMEs not engaging? May not know about them, heard things from their friends. Knowing this might help us help them. i.e. cyber essentials – only companies bidding for government contracts

Ann – Tricky from university perspective.

Nikki – Her and husband have SME, difficult for someone who knows about cyber security, would be very difficult for people with no knowledge.

Paul – May ignore security measures until there is a problem – human nature.

Cheryl – Was surprised in work with SMEs that they didn't have it. To SMEs this is not normalised. Need to normalise something you wouldn't come across.

Matt – SMEs don't employ people to outsource – health and safety, tax, etc. Since don't have to deal with cyber safety in law, don't do it.

Sarah – Need knowledge about what they should do.

Jo – Stakeholders?

Sarah – Larger organisations all have corporate responsibility on agenda, is there a way to have them help smaller businesses?

Paul – Some suppliers will only deal with them if they have some things in place.

Ann – How good and useful is info on cyber security? Could universities help? They will have a significant amount of knowledge.

Paul – Banks could help.

Cheryl – Vulnerable areas – SMEs but also small charities. Not regional charities, but small ones. Current government encouraged local groups to come together and create charities. Requirements were all financial, needs to be guidelines surrounding security. Micro-businesses under SMEs also vulnerable.

Ceri – Where do they get the best advice from?

Cheryl – Would be interesting one to research. Getting general advice from huge variety of places.

Paul – Small businesses may give PowerPoint once a year – can tick the box.

Jo – Academics asked to ask how small business leaders learn. Found that they learn primarily on the job. Can't tell business owners how to run their business as so diverse.

Ann – More of an action-based approach.

Paul – Finding which bits make people wake up and acknowledge they could be next. What works in driving awareness and supporting change? People who work for the businesses often involved in security breaches.

Jo – Who are people doing this?

Paul – Chances are they're younger, have more knowledge.

Cheryl – May be that businesses can't afford background checks of employees. Sometimes they pair up with larger organisations, but not always effective. Comes down to a trust issue – must trust organisations you're working with.

Jo – Who would be interested, engaged, specifically in your current networks?

Paul – Someone from Humberside who works in cybercrime, interested in looking at research surrounding small businesses. Chris Wright.

Jo – China/ Export group.

Sarah – West Yorkshire Crime – affiliates here could be interested.

Cheryl – NESTA – interested in development of new products.

Ann – NESTA has applied element over process of innovation. Bigger banks could chip in a bit.

Nikki – Usually people from bigger organisations – not sure why people from smaller organisations don't hear about it. Info Security Group in Manchester that exists for information sharing. Free. Smaller organisations could latch onto this. But how do you get info out?

Cheryl – Many businesses based in rural neighbourhoods.

Nikki – Usually in big cities, so people who work in big city go, not smaller organisations.

Ann – Where does money come from? This strikes her as an area where money would be available. Home Office could get involved if it's built into their priorities.

Jo – Horizon 2020 – European program for research and development. Lots of dimensions to Horizon 2020.

Paul – Cyber security info partnership – run by Adam Beaumont. He said if anyone wanted help he'd be happy to provide support.

Jo – He has connections in university. Important to understand other networks even if aren't involved in those that aren't as vulnerable.

Sarah – Digital Eagles – Barclays.

Paul – Shouldn't be policing demand – about empowering people to protect themselves and police will be there for those that have done all they can and couldn't manage.

Cheryl – This is very hidden, harder to be well informed.

Paul – Businesses go down because of this.

Cheryl – Political dimension to it.

Paul – Benefit to get businesses contributing to economy.

Ann – Where info about threats come from – IT department at big organisations (small organisations don't get this) and social media/internet.

Cheryl – Almost a public health issue

Jo – Resources required.

Paul – Role to play with police and crime commissioners.

Ann – Intro of enslavery act(ph) – has implications for smaller businesses. Sometimes bigger businesses don't do things they're supposed to unless they're compelled.

Sarah – Needs to come through national steer. Protection and empowerment needs to come from top level.

Nikki – Needs to filter further down from big organisations. People aren't always victims with cyber crime, sometimes didn't step up and do what they should.

Paul – People are willing to comply with regulations – better if they're in place.

Cheryl – Must be achievable, manageable.

Ann – Some incidences in which regulations and changes to law happen as a result of universities and other partners.

Cheryl – Interviewed nearly 60 mentors to small businesses, not coming from them. It's invisible.

Jo – Practicalities in terms of next steps?

Cheryl – Find out what's already out there and if there is information, why are we perceiving that no one is doing anything about it?

Jo – How reasonable would a scoping exercise be? What's out there in terms of academic understanding, grey literature, current policing?

Paul – Federation of Small Businesses do annual survey nationally – some cybercrime material in there.

Matt – Wider scope than Chamber of Commerce.

Jo – 1a – scoping what's out there, 1b is vulnerable groups. 2 is barriers. 3 is action learning sets – issue, learn/change/review

Matt – So much business crime not reported to police – more not reported than are.

Ann – There has to be a neutral benefit in partnerships.

Nikki – Government publication lists top threats.

Jo – Anyone keen to take this forward?

Ann – Theoretically quite keen, but somewhat outside N8 – up for a lighter touch relationship.

Matt – Field isn't just cyber, element of my work. Do have interest, but must give it some thought.

Jo – Funding is available from N8, but must fit needs of partners around table.

Paul – Can talk to force and firm it.

Sarah – Sure people in force might be interested, have to talk to them.