Uncertainty & Complexity in the Internet of Things:

Analysis of the IoT Smart Family Workshop
London, 24 May 2018

INTRODUCTION

The Research Institute in Science of Cyber Security (RISCS) is the UK's first academic Research Institute to focus on understanding the overall security of organisations, including their constituent technology, people and processes. RISCS is focused on giving organisations more evidence, to allow them to make better decisions, leading to the development of cybersecurity as a science. It collects evidence about what degree of risk mitigation can be achieved through a particular method – not just the costs of its introduction, but ongoing costs such as the impact on productivity – so that the total cost of ownership can be balanced against the risk mitigation that has been achieved. RISCS's main goal is to move security from common, established practice to an evidence-based practice.

On May 24, 2018, RISCS held a workshop in London that looked at highly complex decision-making. It followed on from the previous day's look at the utility of cyber security metrics. On Day 2, we asked, "What happens when levels of complexity and uncertainty go beyond the capabilities of cyber metrics?" We began with some presentations on techniques for orienting ourselves in complex problem space before embarking on the workshop.

We would like to thank all the participants for their time and input and we would also like to thank the research team from the Digital Policy Lab at UCL STEaPP for helping to design and facilitate the workshop. A special thank you to Dr Ine Steenmans, whose Smart Family concept formed the basis of our workshop.

For further information about this report or about other RISCS initiatives, please contact Emma Bowman at riscs.administrator@ucl.ac.uk.

METHODOLOGY

To immerse ourselves as group in a complex problem space, we explored the topic of The Internet of Things. Specifically, we used the concept of the Smart Family in the year 2030. Consistent with the founding philosophy of RISCS, we took an inter-disciplinary approach, exploring eight personas which each play a crucial role in the IoT problem. We asked ourselves, ***"How do the various disciplines converge their interests to bring genuine benefits from IoT technologies to strengthen and support the smart family unit?"***

We introduced eight personas:

- Consumer
- Technologist
- Manufacturer
- Financier
- Security Expert
- Policy Maker
- Academic Researcher
- Mischief-maker

We gathered a group of 50 or so people from academia, industry, the policy community and the technical community. We asked these people to self-identify themselves under these personas, for which separate tables were provided. Working in groups, people were asked to explore the following questions:

- my goals/motivations are to…..
- the aspirations for the development of the IoT, which I focus on are…..
- my fears/concerns are….
- 'Key Security Alert': From my perspective, an alert or key take away is…
- 'Time Machine': if I could tell my 2018 self something, it would be…
- 'Crystal Ball': to understand our future behaviour, we need to know […] now

Several scenarios were then presented to groups for their reaction. They were permitted to discuss as many of the following as they wanted, or as time allowed:

- Consumers are exempted from all security responsibilities, with regulation shouldering the entire burden for protecting the citizen. What challenges and issues do you see potentially arising? Would consumer exclusion from security breach liability affect you? How? In response to this scenario occurring, what would you want to do, or who would you want to engage with?
- What challenges would arise for your persona if voluntary Secure by Design standards were implemented by manufacturers? Is there anything you believe is not yet part of that debate? Who do you think should be responsible for implementing these SbD principles? Who would you think was liable if the collective IoT system makes a harmful decision?
- In the future, Internet Service Providers will sell consumers product bundles which include home IoT capabilities that are not specifically requested nor well understood by the consumer. Would you have any concerns with that model becoming the norm? Would you like to see this scenario occur? Why? Are there any potential consequences that concern you which have not yet been discussed?

- What in your opinion are the new, emerging types of harm? For example: social, health, psychological, economic, physical, infrastructure, etc

A spokesperson from each group was then asked to deliver a three-minute read-out of their persona's responses to the above provocations. Afterwards, groups were given the opportunity to mull over their roles in the wider context, with the following questions to guide discussions:

- What narratives should be challenged?
- Where are there conflicting long-term interests?
- What types of security incident do you think will eventually be addressed as normal business?
- Where are we at risk of treating emotions as 'noise'? (This refers to the CRUISSE presentation in which David Tuckett talked about the legitimacy of emotion in decision-making)

At the end of the workshop, all participants were asked to fill in a feedback form containing the following questions:

- What will you take from today? What from today has relevance for your role within the development of the IoT and its security implications?
- If anything, what from today did you find novel?
- What do you need in order to become further involved in the ongoing national discussion on IoT security?

PERSONA STORIES

Consumers

Consumers were concerned about the question of privacy as well as the loss of choice. They focused on the effects on different demographics in society. How was this grand plan going to encompass the poor and elderly? Will they have to buy cheap, insecure devices? What will it mean for people without digital skills? Or people who don't want to participate, yet don't deserve to be disadvantaged by not doing so?

Another big question which sprang to mind was, "What sort of IoT would a smart family actually want? What leads them to purchase a device?" Consumers must first and foremost benefit from the IoT. It must bring some genuine value to people's lives. For example, can the IoT open up previously unexplored options for people, such as a broader range of career choices?

The providers and the advertisers are of secondary importance; the benefits must be shared out equitably. Consumers can see how IoT manufacturers might use enticement to exploit vulnerable people, for example with a smart vacuum cleaner like 'Roomba' potentially saying, "Daddy, if you don't buy me this upgrade, I will die!" This will create pressure on people and produce new forms of harm.

Thus, for consumers, the IoT brings benefits that can lead quickly to dependence or have qualitatively very different impacts on different people. Marketeers may try charging different prices for the same thing. Consumers shut down that line of thinking.

Consumers also feel exempt from security responsibilities. They consider security and safety to be manufacturers' responsibility. Manufacturers should also guarantee that software and hardware is maintained and updated. Consumers want to see laws and standards developed that protect them, not unlike what they've observed in the automotive industry. Insurers may also have a role to play and can incentivise good practices not only within the insurance marketplace but with policy holders themselves.

To achieve all this, consumers were happy to participate in a subscription-based service model (i.e. sharing, discarding, re-selling, rotating devices etc). This would help them protect themselves from the responsibility of maintaining these systems. However, there are concerns that this model presents the risk of excessive e-waste and the over-usage of scarce resources.

Consumers thought about how societal norms could change as a result of IoT proliferation. Would people just get used to being recorded in their own homes? Would having to issue commands to turn on/off voice recording actually become a nuisance, so recording stays on by default? What if you are forced into moving into a flat (e.g. social housing) with IoT devices pre-installed that you don't want? How will you be able to respond?

And given that we are already seeing children today becoming de-sensitised to an emerging culture of surveillance, what will it be like in 2030 and what are the potential harms posed by extreme cases of de-sensitisation?

Technologists

Technologists are of course passionate about creating new technologies. They want to make money and design in efficiency to keep costs down. They get a huge kick out of breaking new ground. They get pleasure from taking an exploratory approach, they love playing with technology. But ultimately

what they're looking to deliver are things that shape the world, providing freedom and empowerment to humanity.

Just like consumers, they don't like having their personal data floating around and they understand all too well how that can lead to a loss of control over oneself and one's identity. They wish to protect both themselves and consumers from the liability for security incidents. After all, it's usually when technologies are marketed and productized by the big service providers and re-sellers, that security vulnerabilities creep in.

Technologists would tell their 2018 selves to spot trends in consumer appetite for certain technologies. They'd capitalise on those trends to develop popular services, but also to amplify the benefits of their innovations for mankind. They would also tell themselves to spend more effort balancing the security of their technologies with the way those technologies go on to be provisioned by system integrators.

Technologists enjoy developing technologies and sometimes the complex human factors around the edges can be tiresome, stifling their creativity and the design of their creations. In a world where consumers are completely exempted from security responsibility and liability, technologists were wary that the burden might fall to them, making design choices more difficult and putting them under pressure to make assumptions they didn't necessarily have the knowledge to get right. Liability issues were surely the purview of lawyers, manufacturers, system integrators and policy makers?

In the scenario where secure by design principles were adopted, technologists wondered about the granularity of the principles. Would they be feasible? How long would it take to establish standards, and would those standards stand still long enough to design something around? They would have to be outcomes focused, agnostic of specific technologies, and reasonable. There'd have to be the flexibility for standards to move with the fast-changing technology landscape, or things would start to get tricky.

Manufacturers

Manufacturers were naturally motivated to reduce their costs while increasing their revenues. They wanted to understand and create demand quickly and relentlessly, then control it. In the future, they expected to see a detachment between suppliers and their perceptions of the consumer need. The data will provide a clear picture of consumer needs, and there is the potential to automate manufacturing processes to respond with immediacy. In essence, supply will satisfy demand dynamically, with IoT on production lines actuating production – even changes to product design – based on sensory data received from within the consumer environment. Innovation will become less about a specific widget and more about how to leverage ever more utility from existing sensory capability.

The key security alert is that the most costly attacks will not be on consumer data but on data flows which exist in the machine-to-machine communications which enable dynamic, automated manufacture. Commercial sabotage could become much more commonplace when systems become so complex as to make attribution virtually impossible. A.I. will be making ad-hoc decisions in real time, based on multiple feeds of data. Detecting the root cause of a serious disruption will be hugely difficult. Manufacturers wanted to tell their 2018 selves to get real assurance in the security of their offerings. Do these things do what you think? Don't use the proxies of security (schemes, frameworks etc), but really test them out on your own terms.

Looking into the crystal ball, manufacturers wanted to prime themselves to move quickly, to fail fast (and cheap), and to keep reinventing until hitting on the killer product. In the scenario where consumers were exempted from all security responsibilities, they felt a key concern was that consumers may become detached from the providers of the smart experience. Consequently, cyber criminal organisations could be manufacturers without any other part of the supply chain knowing.

There wasn't any alarm at the idea of voluntary adherence to frameworks. Manufacturers would evolve and adapt. The priority would be shaping security regulation to strike a balance between protecting their own products from sabotage while maintaining an offensive capability. In terms of emerging threats and harms, competitor sabotage was again raised, as was the possibility of ransomware. Imagine if your washing machine stopped working with all your soapy clothes inside. Annoying, but perhaps a small payment might be preferable to the hassle of rinsing and drying them by hand. Another, quite nuanced, concern raised was about 'training' inputs. If manufacturers don't get to see – or indeed understand – the training data which the A.I. hones itself on, how do they know their intellectual property is actually delivering for them?

Finally, manufacturers touched on the issue of catastrophic systemic failures. How reliable and resilient are systems which are too complex to understand? When policy is code, and dynamic policy is dynamic code, if trusted data is faulty, how do you apply quality control over the manufacturing process? Furthermore, if systems on which people are highly reliant fail, who bails out society? Too big to fail? Or what happens when safety-critical actuation is skewed by missing or corrupted data? And how to we cope with "bubble phenomena", when complex interacting systems cause spikes, which in turn cause disruption, before they return to normal patterns of activity?

Financiers

Perhaps unsurprisingly, those who are actively looking to finance IoT, or expand their enterprises into IoT, are keen to maximise return on investment, monetise data wherever possible (and legal), concentrate wealth towards their own sphere of influence, and develop user dependency on their product lines.

Financiers aspire to maximise perceptions of convenience among target consumers, through marketing. They closely observe emerging regulations and seek to influence any which may saddle them with cost. The moral hazard of being 'too big to fail' can also be capitalized upon, so the risks of growing big and fast can potentially be transferred to the state.

Fears and concerns among financiers included a lack of procurement choice around component technologies. So, while they seek to develop a monopoly for their own products and services, it is unwelcome to have monopolies further up the supply chain, and the risk emerges of being excluded from a monopoly or that your supplier becomes a competitor through vertical integration. Fears listed by financiers were numerous: as traditional currency is gradually replaced by data – and the trading of data – the finance sector may lose relevance and it may become more difficult to maintain influence over the traditional instruments of finance. And with many specialist technologies emerging from SMEs, there were concerns that the bar of entry to market was becoming lower, bringing in unwelcome volumes of very agile competition. Finally, with a very diverse ecosystem of different technologies and protocols, financiers noted there may be increased difficulty and complexity in scaling up services to high levels of profitability.

A big takeaway seemed to be that although the market for genuine security remains unclear, the *perception* of security was what was most desirable for financiers. They would tell their 2018 selves to invest in the "right" stocks and watch closely which firms succeed. In the meantime, amassing intellectual property and data appeared to be a safe bet. In terms of the issues arising from keeping

the consumer exempt from security responsibilities, financiers would look to transfer as much liability as possible through cyber insurance policies (maybe spreading their bets across several policies). Adoption of secure by design principles were seen as advantageous if financiers could get their interests represented at the drafting stage to shape regulation. However, with some of the smaller actors being more agile at engineering security into their products, that could pose a threat to financiers looking to invest in the large-scale enterprises. Similarly, in a market saturated with large vendors peddling packages of both wanted and unwanted capabilities, financiers saw no threat if they were backing a successful player. But being outside that would raise concerns around a lack of diversity in the marketplace. Also, APIs could change unpredictably and affect their product lines, or intellectual property could gradually gravitate into the hands of the big hitters.

Among the emerging types of harm to financiers, crowdsourcing featured as a threat to more traditional forms of investment. Finally, there was uncertainty around investing in firms who carry a lot of unquantified cyber liability.

Security Experts

This group regarded themselves as the middle men. They acknowledged they needed to support a simplicity and ease of use so that security just happens in the background. Consumers should be able to realise the full benefits of the technology without the encumbrance of security. The IoT just isn't going to realise the full societal benefits until security experts can hammer out persistent issues such as flaky software updates and weak authentication. Once security is operating well in the background, it becomes a comfort to know it's there.

Security experts fear the rapid adoption and deployment of cyber physical systems, which integrate several emerging technologies and processes, such as IoT and machine learning. These technologies will collect more and more information about us, and will increasingly make decisions for us. Security experts are wondering: if decisions are made "for" us, will they always be to the consumer's advantage? For example, will models for predictive behaviour lead to us being mis-sold things like mortgages? Who bears the liability for such hazards, especially when adoption of such technologies outpaces legislation? When legal vacuums emerge, the market could quickly become saturated with poor-quality products. What is the responsibility of the security expert in this future? For instance, what are the responsibilities of security experts in a future society that has embraced Connected and Autonomous Vehicles (CAVs), which might require continuous virtual assessment as part of a vehicle's cyber-physical MOT? What role do security experts play in upgrading our existing vehicle safety practices, and what skills do we need to create these jobs in the future?

This led the group to their key security alert: if cyber security doesn't get figured out and consumers become enamoured with ever more advanced technologies (e.g. robot babies as the perfect child), this could have irrevocable consequences for our societies. Security experts asked, "What are the reasonable parameters within which the IoT must operate to protect society?", "What are the minimum expectations of 'good' security? There doesn't seem to be any consensus."

The security experts were wary of everyone becoming overly dependent on IoT, not least because they are unsure of the consequences to the smart family's wellbeing. What standards and regulation will exist, how well enforced will they be? Will regulation ensure that IoT, which increasingly blurs boundaries between privacy, security, safety and resilience, is robust enough not to get it wrong? Will companies be held to ethical standards so that they cannot force unfair terms and conditions on unwitting consumers when influencing them to make purchases?

Will the convenience brought by IoT cause conflict? Will tailored technology erode people's ability to make compromises? Will preference-driven lifestyles begin to cause conflict in the home as

people's different preferences are brought into sharp focus? Could this lead to a backlash, where cyber-physical spaces are vandalised and where important instruments of civil cohesion (e.g. emergency services) are harmed by those resisting technology? What if people start removing wi-fi capability from their environments?

In the scenario where consumers are totally exempted from responsibility for security incidents, security experts were concerned that this would lead to complacence by consumers, who would get no closer to differentiating between the characteristics of security, who wouldn't recognise the early signs of a breach, and who would not develop any instinct for the risks to their home ecosystem by mixing secure and insecure devices in harmful ways.

Finally, in a scenario where security standards existed – which manufacturers had adhered to on a voluntary basis – security experts harboured no misconceptions about their efficacy. Standards are always playing catch-up, and there are invariably major issues with enforcing them. How do you get a set of standards to work flexibly with so many different security issues in play, including resilience, data integrity, reliability etc? And aren't the desired outcomes here a function of organisational culture as much as of technical featuring? There was a sense of urgency among this group: we should have thought about all this earlier on! Ultimately, it was a question of control. The group look on with interest at how case law will begin to address liability for harm caused by complex and interacting systems.

Policy Makers

Our group of policy makers were driven to boost economic growth, to foster innovation, to deliver positive societal outcomes (e.g. better health) and a better quality of life. Minimising harm and maximising social stability were major aspirations for policy makers. They felt that IoT technology could realise these goals by enabling people to work smarter, using time more efficiently and productively. Exporting technology could boost economic growth while also connecting people up to each other for societal good. Public services could potentially be made more efficient through IoT, delivering better value for the taxpaying citizen.

Fears for the future included increased frequency of denial of service attacks, especially those which focused on elements of the critical national infrastructure such as electricity generation and distribution. Societal harms were many and varied, including greater economic and generational divisions in society. Further threats to social cohesion included a physical isolation brought by greater virtual connection (e.g. if the elderly can be treated at home, they miss out on their weekly trip to the doctor, and the social interactions which that entails). All of the above could break down trust between groups of people.

Key security alerts for our policy makers centred around the ownership of data. Who would 'own' data on the citizen's behalf? Who had the right to override control of data? If the state assumed ownership, this might cause snowballing over-regulation, while foreign ownership could also be hazardous. Whichever model emerged, the point was made that monopolistic ownership of data could start to see unwelcome levels of control over people's cyber-physical surroundings. Another concern was that over-regulation of the IoT could lead to perverse outcomes and poor security practices, which could damage the country's reputation as a supplier of quality technology products and services.

If policy makers could tell their 2018 selves something, it would be to spend more time considering the relationship between security and economics. Gazing into their crystal ball, they again asked, "Who has the right to override?" and they conceded that the whole process of policy planning and delivery didn't seem fit for purpose when faced with the challenges posed by the IoT. How do you

develop alignment in such a fragmented environment? How should the machinery of governments, and of their governance, adapt?

Academic Researchers

Our contingent of academics aspire to bring consumer empowerment, to prevent citizens from having their autonomy stifled by negative forces. They believe they have a role in minimizing exclusion, helping IoT to be properly distributed globally, and made as affordable as possible. Academics related strongly to the consumer and to defending consumer rights. The IoT must bring benefit, or any corresponding loss of privacy is without justification.

The academics group asked if the re-use of personal data will be exacerbated by a competition for basic resources in the future. Who will ultimately curate data on behalf of the citizen? And who will ensure citizens are educated to understand the trade-offs between convenience and loss of liberties? How can such messages be articulated? Perhaps in the future, data breaches would become so commonplace that people would become de-sensitised to them and stop caring.

The academics also worried about the government's apparent over-preoccupation with promoting technology for efficiency's sake. They felt their voices were being drowned out by big business and that corporate influence over government might be denying us all the opportunity to look at where society is ultimately headed. What would it take for Government to step in and act in the public interest? What sort of threat to national stability (e.g. transportation disaster or similar) would prompt Government to beef up regulation to better protect the citizen?

Our academics felt threatened by the speed of technological development. Some felt that technology moved too fast to enable them to identify or predict new harms. Multi-disciplinary thinking was clearly the way forward, yet multi-disciplinary research still meets with resistance within academia. Academics would tell their 2018 selves to stick with multi-disciplinary research to attain rewards in the long term. However, they wondered what key topics ought to be researched right now in order to bring benefit down the line? They conceded that regulation would always be playing catch-up, so in what way could academia lead the way? It was felt there was a very real threat that large corporations would continue to amass data and use it to produce "evidence" that was more timely and appealing to key audiences than academics' own, more impartial, brand of research.

In terms of a unique selling point, ethics has been – and continues to be – a strong motivator for many academics. Was this the key to moving forward at pace? In any case, the academics felt they were at a pivotal point: reinvent themselves or face extinction. "What career paths will be available to academics in the future?" they wondered.

Key harms identified by this group centred around social harms and loss of control: forced implants, mass-decision making, re-use of data in inappropriate contexts, algorithmic justice, all culminating in a loss of value in the individual.

Mischief Makers

Unencumbered as they were by legal or ethical constraints, our mischief makers saw most things as an opportunity. The odds are always stacked in their favour; the red team just needs the blue team to make a mistake now and again. Data could be monetised in a variety of ways, while certain attacks could be crafted to have quite considerable influence, e.g. politically. The mischief makers are mercurial creatures: a sense of disapproval or revenge could motivate an attack such as corporate blackmail, while a sense of injustice could motivate them to act philanthropically. They also talked about patiently laying the groundwork for an attack, for example the careful

reconnaissance required to deliver a good “spear-phishing” email, or the building of their global reach to attack the ‘edges’ of the internet.

Mischief makers always like open standards and interoperability, with all the transparency that brings. Unmanaged devices are always handy, so they don’t like easy or affordable ways for people to lock down their endpoints. Concerns for the future included getting caught and losing sight of their targets. Mischief makers would tell their 2018 selves to keep promoting open standards, to ruthlessly identify and pursue the weak, and to look at all the things that are *not* happening: which problems are not being solved? Which vulnerabilities are being forgotten about while attention is drawn to the trending security issues of the day? Gazing into the crystal ball, the mischief makers noted that it might be wise to avoid using wearables or other trackable IoT now, as in the future that data might be exploitable by law enforcement and might hamper their ability to operate with stealth.

In the scenario where consumers are exempted from security responsibilities, mischief makers saw an opportunity to zero in on specific target groups whose user needs might not be benefiting from regulation. The fact that liability for security breaches rested so heavily with operators prompted this group to think that security operators themselves might actually be motivated to make mischief on occasion. If consumers were protected from any liability, this might attract more consumers to the marketplace, which would of course bring greater opportunities to mischief makers. And if levels of state control were high, then this would simply motivate some mischief makers to make more mischief, challenging the state to keep up with the myriad techniques for undermining consumer confidence – and even citizen perceptions of national stability?

In the scenario where secure by design standards were made available for manufacturers to adhere to on a voluntary basis, mischief makers readily saw the opportunity to exploit any lack of understanding or any erroneous implementation of such security principles. It was win-win whatever transpired! In response to the scenario where large vendors were saturating the market with unwanted IoT functionality, the mischief makers saw the golden opportunities presented by vulnerable technologies being present in people’s homes! Lots of money to be made, lots of wholesale disruption to be waged, if that was the order of the day.

The main fear for the future was that the tools of cyber mischief could all too easily be turned against mischief makers, perhaps by other mischief makers but also by the state, using mischief making tools under special laws.

APPENDIX: PARTICIPANT FEEDBACK

What will you take from today? What has relevance to your role within the development of the IoT and its security implications?

- "New insights and considerations regarding potential implications (opportunities and risks) of a broadening IoT."
- "I am unsure of my exact role in the development of IoT, but will bear in mind how my own research may apply and relate to this new domain in the future."
- "Surprised that there seems to be a belief that that IoT is a good thing."
- "A view of the wider issues of trying to consider the possibilities and pitfalls of attempting to 'future proof' currently new technology. The understanding of the lack of knowledge about where and when models will be relevant."
- "I now have a much clearer understanding of how manufacturers view this problem."
- "The importance of focussing research on potential leverage topics – areas you can influence and have potential to change outcomes."
- "Need to consider socio-economic and psychological aspects."
- "That there is a national/international group discussing the issue of IoT security. At some point there will be useful/practical guidance to assess IoT security risks."
- "There is no single solution that fits all. Users should be given the flexibility/choices to fit their particular needs/circumstances."
- "How difficult it is to deal with uncertainty. How interesting and contentious policy experiments are."
- "Some really interesting questions… that we didn't have time to explore properly. It's hard to think long and out of the box, but diverse experience or opinion in a group helps."
- "Move to personalised virtual space than physical space = go to the pub, don't like the environment, change your reality automatically (IoT changes it for you, xxxxx you don't like it."
- "The IoT may be perceived as new but we are still trying to describe it with old metrics which never described security anyway."
- "The simplicity of (low level of) current discussion. Look at awareness of similar challenges in other sectors."
- "Variety of points of view on a multifaceted topic. IoT are expected to have interaction with medical devices, therefore security implications are of paramount importance."
- "It was very useful to network with the wider IoT community, especially when there are complementary strands of work taking place."
- "I don't feel that this workshop addressed the challenges of the 'now' state and then how we move to 2030. I think there needs to be work looking at the standardisation of security for IoT devices. Maybe a new ISO standard?"
- "The opportunity of having discussions with such a wide variety of people with their differing perspectives, opinions – positive and negative – that assisted me with building (rapidly) a novice to this area."
- "It was extremely stimulating and I felt 'safe' within this environment to be honest about my lack of knowledge/experience of such subjects."
- "Need courage to make decisions to address 'complex' policy problems like IoT security."
- "Some more examples of where we have a huge research deficit."
- "That IoT is only a tiny part of the larger national/international narrative and this has two consequences:
  - If you think small you miss the bigger issues;

- If you think large it's impossible to really get started"

- "Different narratives and perspectives that are not security related to encourage different parties to take an interest in security: their market drives and priorities."
- "Finance drive is completely separate drive from security and that can sit across security needs/don't-haves."
- "Future looks – we think too currently and don't prepare enough for the future."
- "I'm going to take back some thinking to the NCSC – particularly the assurance space and how we gain confidence now and in the future. I shall position our research to address the problems that have been discussed – an agreed problem book?"
- "Representation of security risks depends on company culture."
- "Decisions are based on emotion so logical stats are only a part of the input to provide."
- "Great talk on uncertainty this morning. Relevance to me is discussions around shape of government need for an IoT future that is increasingly decentralised. What governance means in a complex world where things cannot be 'controlled' also relevant on an organisational level and team level etc."
- "Communication: mapping technical concepts to social concepts; shifting patterns of responsibility – individual, corporate, government; risk."
- "The importance of trust and implications of it breaking down in any of the key stakeholders together with the complexity of the eco-system. Very relevant."
- "Increasingly worried about the degree to which this pathway is seen as inevitable – what are the alternative scenarios and how might they come about? (How) will it be possible for individuals to opt out (if at all)? What would be the points of no return? When does it become too big to fail (and what are the consequences of that)?"
- "Complexity manifests in different forms but it tends to get articulated, driven by interests. So as someone who works with policies and standards, experimenting with approaches that answers to collective interests/balances competing interests to build into security standards is important."
- "Greater understanding of complexity."
- "Uncertainty is a nice lens to consider strategic aspects of security - nice provocation."
- "Varied perspective on engaging in active and prescribed security reminded me that I need to adapt thoughts / actions etc."
- "That we are still looking backwards in understanding the IoT and failing to understand that it is fundamentally a machine to machine concept."
- "Social and psychological perspective on cyber security is really important. Too much focus on small-world optimisation at expense of 'good enough' adaptable approaches which consider context."
- "Clearly there are huge uncertainties about the status of security in the future. I need to strive to proffer solutions that create a balance between the services of my product and the security issues involved."
- "Has led to a number of changes in the approach we will have to take in the future."
- "There is a great uncertainty in IoT that needs response/input in making it resilient. The exploitation of weakness and vulnerabilities emerging from IoT automation is relevant to my role."
- "The complexity and diversity of the cyber security challenge."
- "Secure by default; don't leave consumers to take responsibility to secure IoT."
- "Whilst future challenges are unknown, a trend in technology that we cannot control (e more data being captured about us, such as through smart meters) can be guessed. How people will

react to this, however, is unknown. Capturing people's feelings when the feelings are uncertain. They don't fully understand the root of the situation but can provide a vague description of it."
- "The wide spectrum of views and perspectives even in a room with a-priori common interest."
- "That attempting to make decisions under an uncertain set of circumstances should be acknowledged as reality. Looking at different models beyond the 'measurement/metrics' which we discussed yesterday."

If anything, what from today did you find novel?

- "The insights and discussion points raised from those coming from other disciplines."
- "The level of general acceptance/expectation that IoT is not a fad and will become an essential part of everyday life."
- "Other ways of looking at risk."
- "Being able to look at realistic but seemingly crazy scenarios."
- "Smart Family is a great new concept for me."
- "Having a framework to use for horizon-scanning."
- "The nature of uncertainty in systems."
- "Trying to get the perspective from different hats/personas."
- "Being forced to attend to different perspectives"
- "The amount of structure to the workshop…. It helped but did stifle interesting conversation a bit."
- "Finding elements from my PhD (2011) are embedded in the discussion areas and have the potential for further development."
- "The strength of belief that a truly secure system can be built."
- "The decision making process/theory when it is ruled by uncertainty in all forms (technology, social aspects etc…)"
- "The workshop was a different way at looking at the problem, just in the wrong timeframe. Maybe a red teaming workshop, based on the cyber attack kill chain, based on a smart home/smart city could be useful."
- "Interesting to see that most of the discussions were based around the technology; it was a useful point to start considering the 'emotional' impact. The technology would not happen without the human element, unless of course the time comes where it takes over!"
- "That IoT is redefining the UK's democratic basic (central government vs devolved/local government)"
- "Finance perspective to back any company/portfolio of companies in order to reach an overall profit rather than focus on a company's individual outcome."
- "Future look."
- "Community and diversity of thinking."
- "Very real risk of failure of a whole category of valuable innovation (Hindenberg)."
- "I liked the use of different perspectives from different players. It would have been good to mix people up so they had to consider things from a perspective different from their day job."
- "Great to hear from range of experts in different sectors about their top concerns / hopes for the future of this area."
- "How IoT challenges existing gov machinery."
- "The multi-dimensional / actor approach."
- "The notion that emotion and cognition are intertwined (not necessarily novel to me, but hardly ever mentioned in the context of ICT."

- "(personal data security) apathy and resistance."
- "Not sure about novel, but the frustration from some practitioners at the insistence of clients on focusing on 'small-world' technical issues but avoiding the more uncomfortable discussion about wider uncertainties and context."
- "The complexity involved in addressing security in the IoT environment."
- "Interesting to hear the different (conflicting!) views of those who attended."
- "Challenges associated with IoT."
- "Perspectives from different players in the IoT eco-system (and they need to bridge the gap or fine-tune)."
- "The ability to freely discuss ideas and problems/challenges in the field without it being too structured."
- "The policy experiment that came after a forward-looking set of discussions was very interesting."
- "That models of complexity in decision making are available, even if they aren't 'end goal', they should help us facilitate the future discussion."

What would you need to be involved in the ongoing national discussion on IoT and security?

- "An understanding of attitudes of consumers/the public, in terms of their valuation of personal privacy vs convenience; how this may change/develop over time; or funding to find this out!"
- "An invite! And how this fits with the global view."
- "A specific direction on the case studies and scenarios of concern, and the requirements to set them up/replicate them so we can probe the real concerns. Access to a bit more of the underlying technology/code samples for testing (pipe dream, I know….)"
- "Continued interaction and for IoT to be an ongoing theme in RISCS."
- "Ability to be involved in multidisciplinary discussions/conversations both online (social networks, for example) and in person (workshop sessions like this)."
- "Understand how to modify our current behaviour to take into account the uncertainty of the future. How can we do lateral thinking in a way that is meaningful for the present?"
- "Medical device IoT."
- "Point of view from IoT manufacturers (or participation)."
- "More brain power/more time to absorb the arguments."
- "Nothing …. It's part of my job…. Actually more opportunities like this would help."
- "Funded involvement in a study group to produce White papers in the first instance and settle on the research questions (if we can imagine tomorrow's problems today then they are already problems)."
- "A belief that the discussion was impacting good practice."
- "I am currently involved, and believe that broader participation of all the stakeholders involved is an advantage."
- "Nothing to be involved, happy to be part of the conversation. I think the workshop was a missed opportunity. It should have really focussed on the issues and challenges now (2018) and how we should address them as opposed to looking at 2030. The conversations dived into too many rabbit holes. Challenges are:
    - Getting manufacturers to create devices that are 'secure by design'
    - Authentication
    - Secure communication protocols
    - Patch and firmware updates/management

    - Anti-virus and firewalls at nodes
    - No default passwords and are not sent in the clear
    - Possibly ensure that device names are not sent in the clear."

- "Attending this session has allowed me to network and get to know who I really need to be working with to allow me to get the results I need for my current project assignment – thank you!"
- "There needs to be useful fora for policy maker to engage with a variety of IoT communities."
- "More funding calls and good research questions that I can get other academics excited about."
- "Definitions around and understanding of the layperson's experiences, expectations and the variables that they use in relation to engage purchasing IoT devices – and Feja's comment on the need for interdisciplinary research and community."
- "Consumer groups and market leaders to counter the expert opinion. Representation of the lowest common denominator will help define a minimum requirement that is relevant to all."
- "I am already, but I would want to create a community that was multi-disciplinary and have as many perspectives and possible to take this forward. Is PETRAS already doing it?"
- "Analysis of trust aspects. What do consumers see (implicitly) as their vulnerabilities and showstoppers?"
- "Regular updates by participants from multiple disciplines via short (0-15 min) podcasts. Moderated/balanced content. Guest speakers sharing views."
- "Invitation to events with broad remit but clear outcomes (today was excellent – where does it go next?"
- "Funding for research?"
- "More meetings of an inter-disciplinary nature like this."
- "I am involved! Funding!"
- "A discussion on public awareness of Data Security (to combat apathy) as the market will drive change through demand."
- "To be convinced that we are following a route that under some circumstances could provide a worthwhile outcome."
- "Funding for social scientists to be part of these conversations. Some training in key technical issues to help join the discussion productively."
- "I need to make clear what my interests and suggestions are, in achieving IoT security."
- "Information on what has been discussed unless there is distribution of what other tables discussed then the scope is too limited."
- "How to secure these systems, who is responsible for data collection, etc."
- "How consumer (general public) is aware of IoT security; group /community that you can talk to/discuss with."
- "The mass surveillance that the public has no control over. Personal information is used against them (eg by insurers) – could potentially be maliciously stolen."
- "The policy and legal aspect is the one I would want to be involved in."
- "A better description and clarity/exposition of these different models."