IAAC People-Centric Information Assurance research

Paper 6 - The Government's role in creating trustworthy, safe and secure digital environments

Results from IAAC's PCIA workshop of 14 July 2010

This workshop looked at what the Government could do to make the digital environments the public uses more trustworthy, safe and secure.

Disclaimer: This report is not a record of the workshop discussion. It is, as with previous workshop reports, a digest of the many insightful points made in, and arising from, the discussion. The ideas expressed in this report should not be taken to represent the views of any individual IAAC member or sponsor.

Key messages

1. The digital society is built on open networks and open systems (open in the sense that anyone can sign up to use them). These are not used only for inconsequential activities: some open systems allow people to perform substantive operations such as make anyone-to-anyone financial transactions. Enormous benefits have arisen from this openness, many of which were never anticipated in the early days.
2. Openness breeds crime, and open digital technologies breed e-crime. E-crime is a consequence of the agnosticism of open technologies, lending themselves, as they do, equally well to lawful and unlawful purposes.
3. Where open technologies make a telling difference, whether facilitating e-commerce or facilitating e-crime, is where they enable millions of people to be reached at almost zero marginal cost. For e-crime, this enables e-criminals to generate large aggregate returns from their activities whilst generally keeping the impact of e-crime very thinly spread across the population. For the public at large, e-crime is all but invisible and most people do not feel touched by it.
4. Despite this lack of public awareness, there are still good reasons for the UK to want to maintain downward pressure on e-crime and to strive to reduce the harm it causes. The question is how. The dynamics of e-crime are complex and reach across many aspects of the digital domain. Bearing down on e-crime in one area would, in all probability, lead the criminals to adapt their methods and target weaknesses elsewhere. Bearing down on e-crime in a comprehensive manner would, in all probability, stifle innovation and lead to huge long-term costs.
5. We conclude that, to tackle e-crime further, the UK needs to take a holistic view and to follow a multi-threaded approach built on a wide mix of targeted responses. This leads to the first role for the UK Government as, ultimately, only Government can provide the vision, strategies and leadership needed to achieve such a complex national response.
6. The Government is also one of the actors within the digital ecosystem and, as such, has its share of tasks to undertake in line with the national strategies it develops. These include:

    - Improving the trustworthiness and security resilience of the public sector and open systems the public is exposed to.

      Improvements will come, but only slowly, unless the Government takes action to speed the process. The Government should make a determined effort to raise standards of governance and data handling practice in public sector systems and then encourage the private sector to follow suit.

- Requiring greater transparency and openness regarding e-crime losses.

  The public has a legitimate interest in how commercial organisations respond to e-crime. The Government should consider requiring service providers to provide, perhaps through their annual reports, more openness about the e-crime losses they sustain and more transparency about how they cover those costs. Sarbanes-Oxley has already exposed company shareholders to the subject of corporate risk management. The UK Government should consider imposing a similar reporting requirement on UK companies. Doing this would lead to a number of benefits. These are identified within the body of this report.

- Encouraging commercial enterprises that serve the public to strengthen their social role.

  The distinction between the private sector's commercial and social responsibilities is not as clear cut as some would have it, and most commercial enterprises serving the public recognise that there are social aspects as well as commercial aspects to the way they operate. There is scope for asking such enterprises to make more of the opportunities available to them to contribute towards social goals. This would require a debate within the UK on what was deemed sufficient social benefit to justify requisite corporate efforts. The Government should consider facilitating such a debate so the balance between such organisations' responsibilities can reflect better the interests of the paying public.

- Leading the design of safety nets.

  No matter to what degree digital systems might be made safe and secure, there will always be risks and there will always be innocent people getting harmed by digital attacks and accidents. People need safety nets put in place that will help them limit the amount of damage they suffer when they get hit and help them get back to normal online life quickly. The Government should take the initiative to identify the safety nets people will need and to determine how those safety nets should best be provided.

- Updating legislation to encompass digital goods and services.

  There are some areas of legislation where the positions statutes take with regard to digital goods and services are not always in line with the positions they take with regard to traditional physical offerings. The Government should consider whether legislation that is intended to protect the public currently protects them adequately with respect to the digital harms they might suffer at the hands of others.

- Leading international cooperation.

  Governance, monitoring, and intervention to curtail the worst excesses of Internet behaviour can be conducted only through multi-national cooperation. There is a role for the UK Government in strengthening cooperation and creating substantive action around positions and goals that serve the UK's interests.

7. The Government has a significant role to play within the UK's digital ecosystem but it is not the only player. If the Government is to be effective making digital environments safer and more secure, it needs the other parties within the ecosystem to play their parts too. This means the private sector providing consumers with a range of digital offerings so people can buy the level of safety and security provision they want. It also means consumers engaging more with digital safety and security as a personal concern, and making informed choices regarding the way they conduct their lives online.

Discussion

Open technologies and e-crime

1. The digital society has been built on open technologies: open networks such as the Internet and open electronic systems such as e-mail, web browsing, social networking, and anyone-to-anyone payment systems. This openness has brought with it enormous change, innovation and prosperity, most of which was never anticipated in the early days. The UK especially has benefited.

2. Openness, whilst being the midwife of innovation and prosperity, has its drawbacks. Almost any open technology can be exploited for harmful or unlawful purposes just as easily as it can be exploited for beneficial, lawful purposes. Technology's agnosticism with regard to the purposes to which it is put ultimately leads to the rise of e-crime. E-commerce and e-crime are opposite sides of the same coin. E-commerce arises out of those uses of open technologies that are within legal boundaries. E-crime arises out of those uses that are not.

3. Where open digital technologies make a telling difference, to e-commerce and e-crime alike, is where they allow a massive multiplication of scale at a minimal marginal cost. They allow any organisation to reach out to people and perform a simple transaction, but to do so on a scale of many millions.

   On the e-commerce side, open technologies allow commercial companies to provide simple digital services (for example, an open, anyone-to-anyone transactional payments service) and make only a small charge for each transaction, and yet make large aggregate profits through the multiplier of scale.

   Similarly, on the e-crime side, open technologies allow criminal organisations to launch simple digital attacks (for example, phishing in the hope of occasionally capturing financial account access codes) that usually result in only a small loss to each of the individuals who are taken in (such as a small unauthorised payment that many account holders do not appear to notice) and yet make a large illicit haul in aggregate (billions of pounds per year according to reports) through the multiplier of scale. This scaling allows e-crime to flourish whilst keeping the proportion of people affected small and the impact on those affected small.

4. It is not only the multiplication of scale that helps e-crime to flourish. Another way is where the business models commercial organisations use to support legitimate commercial activities also help society to accommodate the burden imposed by e-crime.

   Whether the impact on the individuals affected by e-crime is financial (e.g. unauthorised transactions) or non-financial (e.g. the shock of having been targeted; the inconvenience of having to reclaim from their account issuer the funds they have lost), the direct burden on each individual affected is usually low. In contrast, the costs to the commercial organisations providing the online services that get exploited by criminals (e.g. the financial service providers) can be large when aggregated over all the customers who are affected by these illicit activities. These costs take the form of the monies service providers pay out to compensate affected customers and the costs of the man-years of time service provider staff spend dealing with customer claims.

   However, the providers are able to recoup these costs. They do this through the charges they apply. A small proportion of the charges they apply for each customer transaction goes towards covering the service provider's e-crime costs. In this way, the business models that commercial organisations have developed to support legitimate business allow the costs of e-crime committed against their services to be spread thinly over the millions of customers who user those services.

5. This enables the current levels of e-crime to be readily absorbed. The commercial returns service providers can get from providing open systems and services is much larger than the aggregate cost of e-crime against those services, and each consumer's share of that aggregate e-crime cost is only one part of the overall cost the consumer gets charged for using those services.

The case for action

6. This suggests that current levels of e-crime appear to be relatively easily borne. Given that, is there a case for the UK putting more effort than it already does into reducing levels of e-crime? There are several reasons to say Yes.

   - The Government has put, and continues to put, considerable effort into getting members of the public to conduct increasingly significant aspects of their lives online, including engaging with local and central government services online. It needs to ensure its focus is not just on getting a greater proportion of the public to go online but includes making sure that those who do go online can do so safely.
   - The threats faced by the public could become increasingly dangerous. As found in the preceding PCIA workshop[1], the increased professionalisation of the attack community suggests that victims can expect the level of personal harm they suffer from digital attacks to rise.
   - If a broader and more diverse range of citizens responds to initiatives and starts to go online, the population's tolerance of current security shortcomings and e-crime losses might shift. Later joiners might include those who are less risk tolerant or less willing to carry a share of the costs arising from previous inaction. This might create pressure for action in the future where there has been little pressure in the past.

   Given these reasons, the Government has an obligation to ensure that the digital environments people enter into are adequately safe, secure and trustworthy for UK citizens. The Government needs to identify steps it can take to make these digital environments safer and decide on the degree to which it should give citizens the responsibility for making their own choices.

The difficulty of achieving effective action

Accepting that there is a case for increasing the downward pressure on e-crime, what type of actions could the Government consider? There are several possibilities, though opportunities are limited.

More secure and trustworthy technologies?

7. As the preceding PCIA workshop has shown[2], the private sector, acting under market forces alone (i.e. without government intervention), has, on the whole, dealt adequately with the level of security threats seen. In general, PCs and smart phones meet consumers' security and trustworthiness expectations.

8. The private sector could, if pushed, do more. Higher security solutions, such as biometrics and digital signatures have existed for a while, though they have not found their way into mainstream consumer products. And ISPs could make their open networks cleaner by, for example, filtering out malware "in the cloud" and disconnecting servers used for criminal purposes. However, such improvements are unlikely to be pulled through more quickly unless consumers demonstrate they have an interest and are prepared to pay.

   Consumers today show little interest in such improvements. On the contrary, people often object to security improvements that impose additional effort or inconvenience on them. In the light of this, technological improvement will be slow and piecemeal unless something significant happens to generate a step-change in consumer interest.

---

1 See the IAAC report from the 29 April 2010 PCIA workshop – Paper 5 in the series

2 Ibid.

Stronger law enforcement?

Given that the fundamental problem is one of crime, it makes sense that law enforcement should take a lead. However, strengthening law enforcement within the digital domain is not without its difficulties.

9. Tracing and identifying e-criminals is difficult. E-criminals tend to be dispersed, often have no offline criminal presence, and often hide behind false online identities. Investigation and intervention is much more difficult for e-crime than for traditional physical crime.

10. A large proportion of e-crime is transnational, conducted across rather than within national borders. Hence, the law enforcement response to e-crime also has to be international. However, the effectiveness of international law enforcement is often limited by the lack of resource and skill found in other countries. Effective action can also be limited by the lower priority less technologically advanced countries tend to assign to combating e-crime. These countries often have other more pressing priorities that need to come first.

11. Targeted law enforcement action within national jurisdictions can sometimes result in yet more of a burden being imposed on ordinary law-abiding citizens. This can limit how far such law enforcement measures can be taken.

    For example, when the funds being moved within financial systems are e-crime funds, their movement is referred to as money laundering. The financial institutions that run electronic payment systems have a responsibility to try to identify money laundering when it takes place. This imposes a cost on innocent people. Money laundering is a specific purpose behind funds movement rather than being a specific type of funds movement, and purpose is often indicated only by the context of the transfer rather than by the specific details of the transfer. Establishing context introduces infringements of privacy. Hence, anti-money laundering efforts impose a cost, a privacy cost, on the innocent. Consequential impacts such as this can limit how far additional law enforcement measures can be taken.

Limiting technological openness?

12. The benefits of technological openness have been enormous innovation and prosperity far beyond anything that was foreseen. Intervention that constrains technological openness has to be approached with enormous caution.

13. Intervention against a new technology or protocol (e.g. peer-to-peer file sharing) on the basis that it has the potential to be used for illicit as well as legitimate purposes would represent a massive shift away from openness. This would limit innovation, and has the potential to lead to significant adverse impacts on the UK in the medium to longer term.

14. Precedents for intervention against specific technological developments do exist, especially where there are obvious and serious harms that could arise. For example, Governments intervene to restrict the creation of new firearms or weapons. However, intervention against specific digital developments would be difficult. It is often difficult to identify the harms that a new digital development might lead to. Preventing harmful uses is difficult to achieve without similarly preventing beneficial uses. And any restrictions would have to be applied multi-nationally if they were to have any effect.

15. As a result, intervention of any form to reduce the openness of digital technologies would be difficult, is unlikely to be particularly effective, and, if it is effective, is likely to come with significant long-term costs.

Giving commercial organisations social responsibilities?

16. The commercial entities within the digital ecosystem tend to be providers of consumer products and services, not of social goods. Their focus is on providing a return for their stakeholders rather than putting money and effort into addressing the unarticulated needs of silent customers. For them to be

required to take an active, rather than purely supporting, role outside their normal sphere of operation, such as their being given a social or law enforcement responsibility, would require a compelling rationale.

17. Many smaller players in the marketplace do not have the capacity to take on such extra responsibilities. Imposing those responsibilities on all organisations regardless of size would favour the larger players in each market sector and that would narrow the marketplace. Imposing them only on the largest players in each sector would lead to criminal organisations migrating to the smaller players.

18. As a result, imposing responsibilities that do not fit within normal commercial models of operation could have unattractive consequences whichever way they are applied.

The role of the Government

19. As this discussion shows, achieving effective action in this digital domain is not easy. If progress is to be made, the UK will have to take a holistic view across the subject and to adopt a multi-threaded approach. Any actions taken will need to be designed carefully. They should not impose costs that the market or consumers will oppose or that would be disproportionate to the harms being addressed. They would need to be well targeted so that they led to actual benefits rather than just shifting the problem elsewhere. And they would need to recognise that the UK's digital environments and ecosystem are global rather than purely national.

20. To bring this about, all sectors within the digital ecosystem will need to work together under a common vision and aligned with national strategies. Only Government can bring this about. The primary role for Government, then, is to provide that common vision, to provide leadership to bring about meaningful change, and to develop appropriate national strategies that reflect the complexities of the subject and situation.

21. The Government is also one of the actors within the digital ecosystem and, as such, has its share of tasks to undertake in line with the national strategies it develops. These include:

- Improving the trustworthiness and security resilience of the public sector and open systems the public is exposed to;
- Requiring greater transparency and openness regarding e-crime losses;
- Encouraging commercial enterprises that serve the public to strengthen their social role;
- Leading the design of safety nets;
- Updating legislation to encompass digital goods and services;
- Leading international cooperation.

Improving the trustworthiness and resilience of systems

22. A trend that has been in evidence for many years and which can be expected to continue is the gradual improvement in the general level of trustworthiness and security resilience of online systems. The Government would do well to accelerate this trend for the wide range of online systems the public is exposed to. These systems include central government systems (such as online benefits and tax systems), public service systems (such as the energy company's application a homeowner's smart meter talks to), national infrastructure systems (such as the retail banking applications people use), and open private sector systems (such as social networking sites and retailer sites).

23. This would need to be led from the public sector. As mentioned in an earlier workshop report[3], the public sector, as the monopoly provider of government services, is in a position of forced trust. It must

[3] See the IAAC report from the 16 February 2010 PCIA workshop – Paper 4 in the series

take care not to undermine that trust. The public sector does not have the luxury of taking quite the same level of risks the private sector can take, and public sector information systems need to achieve higher levels of trust and security resilience than they do at present.

24. The way the Government can accelerate this improving trend is to make a determined effort to raise standards for public sector systems and then to encourage the private sector to follow suit. This encouragement would be aided by the fact that many public sector systems are provided by, or operated by, the private sector. The private sector would be exposed to the Government's raised standards for public sector services and could then be asked to apply those principles to other systems they supply.

25. There is much more to raising standards than simply establishing suitable technical standards and designing in better security. Making information systems more trustworthy and resilient will require higher standards of governance and better data handling practices across all parts of the digital ecosystem. The Government should start by aiming to create a much wider appreciation within all sectors that IA is a necessary enabler of the future UK digital society and can, in many situations, help contain operating costs. It should then aim to create a culture of competence with regard to the handling of people's personal information, within government, within government service providers, and within the private sector. It will also need to effect a substantial change in culture across the whole of the application provider community. Future systems should be designed to minimise the level of trust they need to achieve their functionality and to handle policy failures gracefully rather than simply to terminate whatever operation is being performed.

Requiring transparency and openness regarding e-crime losses

26. Consumers appear to be content with the current practice whereby a service's e-crime losses are shared across its customer population. This might be because they are unaware that they are the ones carrying these costs. They would be unaware of this perhaps due to the lack of openness from service providers regarding the level of losses being sustained, the lack of transparency regarding how those costs are recouped, and because the cost per consumer is still very low.

27. Though this might suggest that current sharing arrangements are sustainable, there is a debate to be had about whether the public at large finds the current level of e-crime losses to be acceptable and whether these losses are being borne in the right place. In responding to e-crime, it is the service providers that decide how much is spent on improving security resilience within systems yet it is consumers who bear the cost of e-crime losses. This gives consumers a legitimate interest in the way commercial organisations respond to e-crime. Consumers are entitled to have a voice regarding whether to continue sustaining the current levels of losses or have service providers do more to reduce those losses.

28. Consumers would need to understand that there is a trade-off being made that could mean they might not want to see e-crime losses driven down to the smallest amounts possible. Steps to improve security resilience can sometimes lead to greater inconvenience to consumers. Security measures impose a "convenience cost" on the consumer when they result in consumers having to undergo more rigorous enrolment, authentication or authorisation procedures whenever they sign up or sign on to use a service. This convenience cost would need to be balanced with the apparent fact that, at present, consumers do not seem to be noticeably inconvenienced by the contribution e-crime losses make to their service costs.

29. If consumers were helped to understand this trade-off, and if the marketplace provided a range of online services with some service offerings being more security resilient than others, then each consumer would have the ability to choose. They could decide how they felt about the current level of losses and which of the two types of cost they would rather pay. Those who wanted to see a stronger stance taken against e-crime and were prepared to pay by accepting more stringent security measures could sign up to the more secure versions of online services. Those who cared less about e-crime and more about personal convenience would be free to do otherwise.

30. To bring this about would require greater openness and transparency from service providers. Lack of openness means that the level of losses is not known by those who carry those losses. Lack of transparency means that the public is not aware of the decisions being made on their behalf by their service providers.

31. The Government should consider requiring service providers to provide more openness and transparency. They could do this by requiring companies to state, possibly within their annual reports, the level of their e-crime losses and how they cover or recoup those losses within their normal operations. Sarbanes-Oxley has already exposed company shareholders to the subject of corporate risk management. The UK Government should consider imposing a similar reporting requirement on UK companies.

32. Doing this would lead to several benefits.

- Shareholders would be able to see the level to which the companies they owned were suffering e-crime losses and how those companies addressed these problems. This would enable shareholders to drive executive action if they felt their company had the balance wrong, i.e. if they felt that their company should be doing more to improve security resilience and passing less of a burden on to their customers.

- If consumers were made aware of the losses they cover and that the cost of the convenience they desire so much is higher than otherwise levels of e-crime, they might engage more with security as a personal concern. This heightened engagement is a necessary prerequisite to changing the public's views of, and attitudes towards, digital safety and security risk, and of changing people's online behaviours for the better.

- Greater reporting openness would enable UK law enforcement bodies to get a much better understanding of current levels of e-crime. In the absence of any such reporting requirement, law enforcement is in the dark and unable to prioritise effort, resources and training more appropriately.

Encouraging commercial enterprises to strengthen their social role

33. It is normally thought that the marketplace is not very effective at recognising social goals, for example the social goal (if, indeed, it is one) to reduce levels of fraud, unless working towards that goal can be linked with commercial benefits. If a company can make money from the provision of a social good, then the value of the financial return to the company can be recognised even if the value of the social good to society cannot. Similarly, if a company can make more money investing a given sum in exploiting a business opportunity than in reducing its losses, then the investment is likely to be directed towards the business opportunity. Given these commercial sector dynamics, opportunities to reduce fraud are unlikely to be taken up whilst other opportunities that have a better return on investment remain.

34. The same argument presented in a different way is that it is usually not appropriate for private sector organisations, operating as commercial enterprises, to be asked to take on social responsibilities. However, in practice, the distinction between commercial and social responsibility is not so clear cut. Most commercial enterprises that serve the public do operate under a moral code and display a social conscience. They might be inclined to tolerate a level of fraud within their systems but they are less inclined to tolerate their systems being used for serious crime against the person. For example, ISPs have a good track record of cooperating with law enforcement when it can be shown that a system they provide a service to is being used for serious crime such as people trafficking or paedophilia.

35. This suggests that there might be scope for asking commercial enterprises that serve the public to play a greater role in achieving relevant social goals provided the steps they are asked to take are not disproportionate to the societal benefit. For example, for over 25 years all organisations that handle people's personal data have been required by data protection legislation to contribute to a social good by

making their information systems and processes protective of personal information. If it were deemed proportionate, private sector organisations could, in much the same way, be required to make their digital systems more resilient to e-crime.

36. This would necessitate a debate on what, in the UK, was deemed proportionate. That is, what constitutes unacceptable use of open systems (e.g. using them to distribute child pornography, to launch attacks against the CNI) and what actions should service providers be required to take? For example, should service providers be required to disconnect malware and botnet C&C servers, delete obvious e-mail scams and spam at source, notify customers whose end-user systems are showing obvious signs of having been conscripted into a botnet, and so forth? Or are providers justified in maintaining that steps such as these are more than they can be expected to take and that as providers they have no responsibility for the attacks they allow to pass through their infrastructures?

37. The Government should consider facilitating such a debate so the balance between commercial and social responsibility can better reflect the interests of the paying public, and any impact on the marketplace arising from associated changes could be scrutinised and understood.

Leading the design of safety nets

38. No matter to what degree digital systems are made safe and secure, there will always be some level of risk and there will always be cases where innocent people get harmed by some form of digital accident or attack. In some of these cases, the impact on the consumer might be serious financial loss or serious inconvenience from having their digital identity hijacked or stolen. These can be difficult outcomes for victims to recover from. For this reason, there is a need for the Government to consider putting adequate safety nets in place to catch people when they fall victim to serious attacks.

39. For example, if a person were to become a victim of identity theft, most people would have little idea how far-reaching the affects could be or of what to do to limit the ongoing damage and gain their identity back. An appropriate safety net might be the creation of a network of digital advocates, people who understood how the digital world worked and could work on behalf of victims to help them recover from their attack.

40. As people increasingly adopt digital methods and conduct increasingly significant aspects of their lives online, the public will need suitable safety nets to be put in place. The Government should take the initiative of identifying what sort of safety nets people will need and of deciding how those safety nets should best be provided. This should be an essential part of any plans the Government might have to increase the proportion of public services provided online.

Updating legislation to encompass digital goods and services

41. There are some areas of legislation where it might be appropriate for current statutes to be revised to clarify the responsibilities of those who provide and those who use digital goods and services.

42. As discussed in the preceding workshop[4], the position legislation takes with regard to digital goods and services is not always in line with the position it takes with regard to traditional physical offerings. The example discussed then was where the providers of consumer smart devices are not required to provide products fit for any particular purpose, in contrast to the providers of white goods who are. Twenty or so years ago people typically used smart devices for relatively trivial offline activities such as games and entertainment and writing correspondence that they would then print out and post. However, this is no longer the case. People today rely on smart devices when conducting significant aspects of their lives such as building relationships, managing their financial affairs and interacting with public sector services.

---

4 See the IAAC report from the 29 April 2010 PCIA workshop – Paper 5 in the series

Legislation that is intended to protect the public should protect the public equally with respect to the digital as well as the physical goods and services they now rely upon.

43. There are two other topics that relate to this theme. The first concerns the responsibility of web site providers and application service providers to protect the people who use their systems from suffering personal harm. In the physical world, shopkeepers have public liability should a shopper have an accident and be physically harmed while on their shop's premises. Shopkeepers have been given the responsibility of maintaining a safe physical environment for their shoppers, and have liability if they do not prevent preventable accidents. The equivalent would be to give web site providers and application service providers a responsibility to maintain a safe digital environment for their users and making them liable if they failed to protect their users against preventable digital accidents. For example, they could be made liable for any harm that resulted if they had failed to prevent their sites or systems being compromised and, as a result, allowed their systems to be used to serve malicious malware.

44. The second concerns the responsibility consumers could be given for ensuring the smart devices they use do not cause harm to other innocent people. Dog owners are required to ensure they have control over their dogs, and have liability should they allow their dogs to bite or otherwise harm other people. Given that one person's inadequately secured, compromised PC can cause another innocent person harm by sending out malicious malware, the equivalent would be to give users a responsibility to ensure their PCs do not cause harm to others and to make them liable should they not maintain adequate control over them. For example, if someone were to allow their PC to get conscripted into a botnet and that PC then sent out malicious malware that resulted in other people suffering harm, the PC's owner would be held liable for the harm their PC had caused. It is possible to trace the source of malware to the infected PC that sent it. It would be possible to send the owner a message that warned them their PC was misbehaving and they needed to take steps to get it back under their control. And if the person ignored the warning, it should be possible for action to be taken against them to protect the public from their negligence.

45. The Government should consider whether legislation that is intended to protect the innocent public currently protects them adequately with respect to the digital harms they might suffer at the hands of others.

Leading international cooperation

46. The internet can be thought of as the virtual 'high seas'. Not only are there dangers for people who venture onto the Internet unprepared, but there is also no central authoritative body with powers of enforcement charged with overseeing the Internet and protecting users of it.

47. It would be difficult to conceive of a multi-national body being created to take on that role. Conflicts of interest and differences in priorities would abound. Hence, governance, monitoring, and intervention to curtail the worst excesses of Internet behaviour could be conducted only through multi-national cooperation. The primary example of such cooperation is the European Council Convention on Cybercrime. This came into force in 2004 with the intention of harmonising national laws on cybercrime, strengthening and aligning national investigative capabilities, and facilitating fast and effective international cooperation in the area.

    There is a role for the UK Government in strengthening cooperation and leading substantive action around positions and goals that serve the UK's interests.

48. There are various groupings that could be used to carry forward a digital safety agenda, such as the EC, G8, Interpol and Europol, building on practices of multi-national cooperation already in place. Those groupings based on law enforcement cooperation would, for example, enable the UK and other advanced countries to channel support for building up the law enforcement capabilities of other countries that currently lack the UK's capabilities. Those based on technical cooperation would, for

example, enable the UK and others (notably other EU countries and the US) to federate the national electronic ID schemes they are building.

Other parties to play their role

The Government has a significant role to play within the UK's digital ecosystem but it is not the only player. If it is to be effective making the digital environments the public use more safe and secure then it needs the other parties within the digital ecosystem to play their parts too.

The private sector

49. With regard to the private sector, this means the private sector providing consumers with a range of digital offerings so people can buy the level of safety and security provision they want. This covers not only the smart devices people buy but also the digital environments they use.

50. For example, in some cities where the streets can be dangerous, people have the option (at a price) of living within a "gated community", i.e. living within boundaries where many of the threats to innocent people are kept at a safe distance. The equivalent in the digital space would be giving people the option of connecting to the Internet through a secure network service rather than people having the Internet come right up to their digital front door with the full force of all the threats it conveys. Such a secure network service could, for example, provide users with Internet access through clean pipes, i.e. with malware and malicious content filtering "in the cloud" so users were not exposed to harmful content in the traffic they received. It could also provide hygienic web site access, i.e. access through hardened proxy servers with strong application-level safeguards. Then, if a remote site or system attempted to infect the user's PC with malware or plant a root-kit on a user's system, the attack would get no further than the proxy server at which point it would reliably be blocked.

51. These secure network services would give consumers the option of having a safe channel into the Internet at a price they might be willing to pay. In effect, they would be providing consumers with the opportunity to pay a highly competent service provider to maintain a high level of security resilience in preference to each consumer having to maintain that level for themselves.

Consumers

52. With regard to consumers playing their part, this would entail consumers engaging more with digital safety and security as a personal concern. Consumers need to become more receptive to the wide array of awareness-raising materials they are exposed to, to make informed choices regarding their own online actions and behaviours, and to make informed choices relating to the various safety and security offerings that are available to them. People need to apply much the same level of common sense regarding their personal safety in the digital domain as they do their personal safety in the physical domain. For example, they need to learn to recognise possible scams and not fall for obvious ones, and learn to apply the same level of caution to their interactions with other people in digital environments as they do in non-digital environments.

    The question of how to encourage this greater level of engagement from members of the public is the subject of a later workshop within the current series.