IAAC People-Centric Information Assurance research

Paper 5 - The security resilience and trustworthiness of smart electronic consumer devices

Results from IAAC's PCIA workshop of 29 April 2010

Introduction

The main purpose behind IAAC's PCIA work is to understand how the developing digital society can be made trustworthy, safe and secure. This is so that individual members of the public can feel comfortable participating in the digital society rather than feeling that that is possibly an unwise or reckless thing to do. If people don't participate in the digital society, or rather if their participation remains limited because of their concerns about conducting important aspects of their lives on-line, then enormous opportunities for national transformation and the enrichment of people's lives will be missed.

IAAC's PCIA work over the past year has been aimed at understanding the breadth of issues relevant to PCIA and at outlining a broad approach to dealing with those issues. We have, as well, explored two particular issues in greater depth. The first was the issue of how organisations that gather and process personal information can ensure they do not alienate the people whose data they process. The second was the issue of how those organisations that are custodians of personal information should govern their sharing of that information. The particular focus of that latter discussion was on those situations where the benefit to the public interest being served by sharing is potentially in conflict with the personal interests of the individual people whose information is being shared. Reports from each of the four workshops IAAC has run over the year are freely available.

IAAC's PCIA theme for the next few workshops will be "Helping people fend for themselves online". The purpose of these workshops is to explore how to help members of the public take on the things that they need to do to keep themselves protected online. Our aim is to build an understanding of what issues fall to people to deal with themselves. We will then explore what tools and support people will need to make it as simple as possible for them to take on those issues and deal with them. In broad outline, we will examine the plans other parties (such as the Government and private sector) currently have to address the issues that people cannot be expected to deal with themselves and that therefore fall to those other parties (issues such as providing more security resilient products, combating organised e-crime). This will enable us to see what issues this leaves for people to deal with themselves. We will then look at the types of tool and support people will need so they can reasonably take on these challenges, and suggest how these things can be provided by various other parties.

The workshop on the 29th April 2010, to which this report relates, was the first of the workshops under this theme. The focus of this workshop was on the parties that provide the smart electronic consumer devices that people use in their daily lives such as PCs and smart phones. The objective was to understand what these providers are currently planning to do to improve the trustworthiness and security resilience of their products. This would help us to understand what issues members of the public will then have to cope with themselves and what tools and support they will need other parties to provide.

Disclaimer: This report is not intended to serve as 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 PC industry and the smart phone industry have followed two different approaches to dealing with the threats people face from the use of smart electronic consumer devices. Though ultimately the threats people face are broadly similar whichever smart device (PC or smart phone) they are using, the two

industries' different business models and development paths have led to them taking different approaches to providing security resilience and trustworthiness within their products.

2. The PC industry has, in recent years, been generally successful in dealing with the threats people face. As a result, most people do not today perceive the risks that arise from their use of PCs for personal purposes to be significant. However, that victory has not been complete. There is a part of the nation's PC community that remains significantly vulnerable to a range of threats, and a part of that community that has, at any one time, already been compromised by an attack of one form or another.

3. The level of vulnerability and compromise within the nation's PC community could be considered large or small depending on one's perspective. However, regardless of perspective, it is evident that the level has not been sufficient so far to generate an audible consumer demand for more resilient and trustworthy PC products.

4. Security in the mobile communications sector has been driven largely by the operators' desire to protect their service revenues. Industry participants have cooperated in the development of technical standards for building trust and security resilience into mobile platforms. They have, in this way, been able to develop mobile platforms that have a considerable level of both. As a result, consumers typically do not perceive security risk or untrustworthiness to be at all an issue for their smart phones.

5. However, the increasing professionalisation and criminalisation of those people and organisations who create security attacks means that consumers are now starting to suffer rising levels of personal harm through attacks such as phishing. These attacks are on the rise against both communities, PC users and smart phone users. If this rise continues, it could start to change the consumer's perception of the risks and lead to a number of changes within the digital ecosystem. It is likely that several different responses to this change in consumer perception will occur at the same time, each to a greater or lesser degree.

6. We could see some consumers start to take more responsibility for their own digital safety and behave more securely. The full potential for this change in behaviours to lead to a marked improvement in consumer digital safety is unlikely to be realised without concerted efforts by government and industry to help consumers make this change. A number of possible approaches to this are discussed. Each has its merits and its shortcomings. As no one approach is likely to be sufficient on its own to effect a significant change in consumer behaviours, what might be required is a broad multithreaded approach that brings together all of these suggestions along with the additional steps that would be needed to address their identified shortcomings.

7. We could see some consumers start to give a higher priority to security resilience, making this a buying requirement for the smart devices they use. This would create a market demand that has hitherto been muted. However, the level of harm being caused to users by the rising wave of attacks might have to grow quite high before market forces alone will respond to such a demand. The reasons for this are discussed. A number of ways that the market could be helped to respond to the rising demand without having to wait for harm to reach such high levels are discussed.

8. If the market responds only slowly to the rising levels of harm, we could see the public's attitude towards the responsibilities of suppliers start to change. Consumers might come to feel that product and service providers have a duty to provide products and services that are fit for purpose and that providers should be made liable for the harm people are caused by products or services that fall short. This would bring consumer expectations regarding smart electronic devices more into line with their expectations regarding other consumer products. It might also lead to consumers looking for consumer protection legislation on which they could rely. If current consumer protection legislation did not enable smart device manufacturers to be made liable for their products not being fit for purpose, then pressure could arise for the introduction of new consumer protection legislation.

Discussion

The PC industry

1. The domestic PC ecosystem includes consumers, the PC industry and online service providers (network service providers and application service providers). The PC industry is itself a large ecosystem that includes hardware manufacturers, operating system manufacturers and application providers. Within that industry, trust and security issues play only a limited role.

2. The PC industry is driven predominantly by market forces. Business models are built around the aims of keeping costs down and sales up, working with thin margins of sometimes just a few percent. Any new feature that introduces additional development costs, such as a security feature, will not find its way into mass-market consumer products unless suppliers can be confident it will lead to additional product sales.

Trust and security resilience as issues for PCs

3. The competition between attackers and product manufacturers is dynamic, often referred to as a battle. In the past few years, threats have grown much more sophisticated. Also, consumer exposure to the prevailing threats has grown enormously. This is due to the roll-out of domestic broadband and people spending very much more of their time online. As a result, PCs have had to become much more resilient to security attacks.

4. Anti-spam, anti-virus, firewalls and regular software security patching are now standard security features for contemporary domestic PCs. These features have evolved to the stage where they are now all but fully automated. They serve as examples demonstrating that the market can respond to security needs and can develop security solutions that are cheap and convenient for users.

5. The PC industry has been generally successful in dealing with the threats people face in the sense that the level of security risk as perceived by the consumer does not appear to have had any significant adverse affect on the market for domestic PCs. PC insecurity and untrustworthiness, whilst registering as a significant issue for a small minority of consumers, does not appear to be perceived as much of an issue at all by the vast majority. Many consumers have never experienced a problematic security incident, and find that maintaining their PCs at an adequate level of resilience adds only a minor increment to their total cost of ownership and requires only minimal user intervention. Global spam volumes are high but, on the whole, spam is easily dealt with and causes people very little inconvenience.

6. The PC industry might consider it has been successful but its victory is not complete. The number of botnet computers around the globe is reported to be in the tens of millions and these are believed to be primarily domestic PCs. Also, the results from Microsoft's malicious software scans of large numbers of machines indicate that of order seven in 1000 of the machines it scans are infected by some form of malicious software.

7. Clearly, this means there is a proportion of today's PC community that remains vulnerable to security threats. An unknown proportion of those will, as a result, have been successfully compromised by an attack at some stage. These vulnerable or compromised PCs are not thought to be well-looked-after modern PCs (i.e. machines with contemporary operating systems and contemporary security features that are kept regularly updated by their users). They are thought to come from two other groups within the PC community.

8. The first group is PCs that have contemporary operating systems and security features but that are not kept updated and patched by their owners. These are being allowed by their owners to retain vulnerabilities that the industry provided patches for months or even years ago.

9. The second group is out-of-date PCs, low-specification machines running old operating systems that cannot run up-to-date security solutions and can no longer be patched to make them resilient to contemporary attacks.

10. This suggests that there are a significant number of consumers who are not taking advantage of the security solutions available to them despite those solutions being effective, low cost and convenient. It is possible there are many reasons for this. It might be that these consumers are not aware that their PCs are so vulnerable or might have already been compromised. It might be that they do not understand the consequences that could result from successful attacks. It might be that the inconvenience or harm being caused to those consumers whose PCs have been compromised is insufficient to motivate them to deal with their PC's security shortcomings, or to motivate them to overcome their resistance to accepting personal responsibility for dealing with the problem.

11. Whatever the reasons, neither the high vulnerability and levels of compromise of this small proportion of PCs nor the effort that every other PC user has to go through to maintain the security resilience of their PCs has yet led to a demand for the PC industry (manufacturers or application providers) to create more secure and trustworthy products. Witness the fact that no PC consumer brand has, to date, followed what might be called the 'Volvo' route, building a brand on higher levels of trustworthiness and security resilience. Differentiation between PC vendors has remained primarily on the basis of the reliability of their products and the quality of the support they provide.

12. A noticeable consumer demand for more resilient and trustworthy machines is unlikely to arise, and manufacturers are unlikely to provide security or trust improvements other than piecemeal and slowly, unless something happens to bring about a change in the current market dynamics.

The potential for threats to cause increasing harm

13. One change that is occurring within the domestic PC arena is a rising propensity for users to be caused harm rather than just inconvenience from PC security and trust shortcomings. This rise is growing out of a combination of two changes. There has been a change in the purposes for which consumers use PCs and a change in the nature of the threat.

14. There has been a change in the purposes for which consumers use PCs. PCs have been in general domestic use for about thirty years. For the first half of that period, they were used primarily for playing off-line games and writing personal correspondence. The advent of the web broadened that range of uses, and now the advent of domestic broadband and Web 2.0 has broadened that range of uses even further. Consumers now use their PCs for conducting significant aspects of their lives online, from building intimate relationships with people they have not known before to conducting personal financial transactions and interacting with public sector services.

15. There has, as well, been a change in the nature of the threat. To stay in the battle with the PC industry, attackers, attack tools and attack methods have needed to grow more sophisticated. This has raised the bar for the attacker community, forcing attackers to become more expert. The time and investment required to enable this has led attackers to look for ways to exploit their skills for financial return rather than just for enjoyment. Attackers have become more professionalised, and have developed the more sophisticated business models needed to enable them to take advantage of criminal opportunities arising from the exploit of security vulnerabilities.

16. This increasing criminality of the attacker community has already started to lead to an increase in the amount of harm (as opposed to just inconvenience) caused to PC users. This is seen in the growing levels of phishing that leads to the theft of people's personal data and/or money.

17. If the level of harm consumers face from the use of their PCs continues to rise, it might at some stage reach a point where it starts to affect the consumer's perception of the risk.

The mobile communications industry

18. The mobile communications industry is centred around mobile service operators. Operators generate their revenues from selling mobile telephone services. Most handsets are provided by operators (rather than by handset retailers) as part of a service bundle or are sold as an adjunct to their services by the operators. Hence operators have a significant amount of influence and control over the mobile industry supply chain.

19. Mobile communications is a regulated marketplace. Mobile handsets need to be type-approved, operators need to have licences to operate, and operators have obligations to their customers throughout the lifetime of their service provision contracts.

20. Mobile communications is a rapidly changing arena. The leading wave of change is around the development of smart phones, i.e. phones that can run user applications and can be used for a variety of lifestyle tasks. It is this component of change that is making mobiles a central feature of the digital society.

21. One of the main commercial pressures within this marketplace is time-to-market for new features. Another is the need to make life easier, less complicated and less confusing for consumers. A third is the need to make mobile phones sufficiently secure that operator revenues can be protected.

22. Against the thrust of competition between operators, there has emerged a drive for players within the mobile communications industry to work together. This has served to increase consistency between mobile platforms and to support multi-platform application development. OMTP (the Open Mobile Terminal Platform) is the industry forum for agreeing mobile platform requirements which are then implemented by players across the industry: platform providers (chipset vendors, handset manufacturers, operating system and middleware vendors); application developers; operators.

Trust and security resilience as issues for mobiles

23. There has always been a significant demand for trust and security resilience within the mobile communications arena, driven by the operators' desire to protect their revenue streams. In the early days of the industry, cell phone cloning was a large threat to operator revenues. More recently, the desire to protect high-value revenues (e.g. m-commerce, mobile ticketing, proprietary entertainment content) has underpinned the industry's demand for high levels of trust and security resilience in its platforms.

24. Before the advent of smart phones, mobile platforms were relatively closed and offered little opportunity for hackers to develop malware that exploited software vulnerabilities. Attacks tended to be on the embedded electronics within handsets. This required a large investment in chip analysis equipment and deep technical skills. Success, on the other hand, in the form of creating an effective tool that the criminal could control, could bring large rewards. Hence, the attack community from the start was small, highly professionalised and highly criminalised.

25. In response to this situation, the approach adopted by the mobile communications industry has been technological. This technological approach has focussed on creating a trusted kernel at the core of the handset and of building trust outwards from there. Members of the mobile communications industry have worked together to create a number of trusted environment standards. These provide a trustworthy platform for overlying applications to run on. They also support secure device management.

26. 'Apps' is the term used for the small, platform-independent, stand-alone, task-oriented GUI applications (often web-connected) that provide a personalised experience for the mobile user. Within smart phones, these are the applications that run on the mobile platform's trusted environment.

27. For apps to be trusted, then not only does the platform needs to be trustworthy and secure but the apps themselves need to be so too. The industry's approach is to rely on technical standards and code quality to provide that trust and security. The belief is that it should, in principle, be easier to make mobile apps trustworthy and secure than it is to make full-function PC applications so. This is because mobile apps typically have a few hundred lines of software code rather than hundreds of millions of lines of code.

28. The desire to encourage the development of high quality app code across a large community of app providers, plus the desire to prevent the spread of malicious apps, has led to the industry's development of an Application Security Framework. This framework includes a signing scheme for apps and the creation of apps libraries – repositories of signed (and hence assumedly trustworthy) apps.

29. The Wholesale Application Community is a recent (2010) joint effort by more than 40 mobile operators to standardise use of the Application Security Framework and to create a unified warehouse of apps built in accordance with the OMTP security principles.

The potential for threats to cause increasing harm

30. The mobile communications industry has shown that it is possible to make smart electronic consumer devices that are highly resilient to security attacks. The mobile communications industry has been successful against the threats in the sense that consumers do not perceive security risk to be an issue for mobile phones. Only a very small number of people have experienced a problematic security incident, and text message spam volumes are negligible compared to e-mail spam volumes.

31. However, as with the PC industry, the battle against the threats is dynamic and any lead can be lost over time. The industry's publishing of its platform standards is likely to facilitate the writing of effective malware. The creation of consistency across platforms increases the potential returns successful malware writers can achieve. It is, therefore, expected that mobile malware will soon start to flourish.

32. At the same time, the erstwhile security resilience of mobile platforms has led attackers to look to other areas of vulnerability they can exploit. One area that has attracted considerable attention is the users themselves. This is leading to a growth in the number of social attacks against mobile users.

33. These trends together are expected to lead to higher levels of phishing, theft of personal information, data integrity breaches and fraud in the mobile communications arena. As with phishing and related trends in the PC sector, it is expected that consumers will start to suffer increasing levels of personal harm through these attacks. If the level of harm consumers suffer then proceeds to rise, it might at some stage reach a point where it starts to affect the consumer's perception of the risk.

34. As a result, though the mobile communications industry has evolved in a different way from the PC industry, both sectors face the prospect of consumers suffering increasing levels of personal harm through the use of smart electronic devices. This similarity in prospects is only strengthened by the current convergence of the PC and mobile communications sectors. Traditional PC manufacturers are entering the smart phone market and traditional mobile handset makers are putting increasing amounts of processing capability and memory into PDAs and smart phones.

The changes a rise in harm might bring about

35. If the level of harm consumers face from their use of smart electronic devices continues to rise, it might at some stage reach a point where it starts to affect the public's perception of the risk. If the public at large, or consumers individually, start to feel uncomfortable with the level of risk that smart devices attract, that could drive any of a number of changes in the domestic digital ecosystem. For example:

    - Some consumers might start to take more responsibility for their own digital safety and behave more securely.
    - Some people might give a higher priority to security resilience, making this a buying requirement for the smart devices they use. This would create a market demand that has hitherto been muted.
    - Some people's attitudes towards the responsibilities of product providers might change, leading them to seek redress from product providers for the harms they suffer. This might then lead to consumers looking for consumer protection legislation on which they could rely.

36. It is not only the consumer who faces risks. Any insecurity and untrustworthiness of smart devices introduces risks to each of the main parties within the digital ecosystem. Consumers are at risk from the increased levels of harm they can be caused by threats. Product providers (device manufacturers and application providers) are at risk of losing market share to others if they misjudge the consumer's reaction. Service providers (network, communications and application service providers) are at risk if the security or performance of their services is affected by compromised consumer devices, or if they are made liable for allowing attacks against end-users (malware, phishing, data theft, etc.) to be conveyed via, or take place within, their services.

37. As a result, it is likely that several different responses to the changing risk landscape will occur at the same time, each to a greater or lesser degree.

Users behaving more securely

38. It is widely maintained that users would be able to protect themselves better against harm if they could be induced to improve their security behaviours. However, the evidence is that, for many users, the potential for personal harm associated with having a compromised smart device is not always sufficient to induce them to take mitigating action. It is not clear how high the risk would need to become before these users overcame their reluctance to act. The question then becomes, are there ways to encourage or help users to adopt better security behaviours without having to wait for risks to grow to intolerable levels. There are a number of possible approaches under discussion. Each has its merits and its shortcomings.

39. One often discussed approach is to make good awareness and education materials available to a wider audience of users. It is undoubtedly the case that, despite the current availability of good awareness and education materials, there are many users who continue to make poor digital safety decisions. Indeed, there is ample evidence available, especially within the PC arena, to show that, if allowed the option, some users will choose not to take any steps to maintain the resilience and trustworthiness of their smart devices if those steps introduce any inconvenience to the user, no matter how small.

40. However, there could be many reasons behind this type of behaviour. These range from a lack of knowledge and understanding of security matters on the part of users through general apathy and inertia to a determined resistance by some people against taking instructions from outside parties. It is clear that different people have different perceptions of the risk and different attitudes towards making themselves secure. It should not be presumed that the only reason people make poor digital safety decisions is a lack of awareness or knowledge. The wider distribution of awareness and education materials is likely to form part of the required response but will need to be accompanied, if not preceded, by separate efforts to address the 'anti-security' perceptions and attitudes some people hold. Experience shows that one does not change people's risk perceptions and security attitudes simply by giving them more information about, and a greater awareness of, risk and security matters.

41. A second approach is for providers to do more to make user security decisions as simple, natural and fitting as possible. For example, suppliers could develop more sophisticated policy approaches that would make it easier for users to exercise their desired level of control over their smart devices. Current practice is typically to give the user technologically-oriented binary options that many users find difficult to understand. Also, the typical response an application takes when it comes up against an inconvenient policy barrier is for the application simply to terminate what it was doing for the user.

42. It could help users if suppliers were to develop approaches that would allow the user to express their digital safety preferences in a natural language form. A policy management layer could then be implemented between the user interface and the platform API that would decompose the user's stated preferences into a set of technical preferences that the platform could then use to control what use applications could make of the device's underlying features and facilities. However, for this approach to work, it would be necessary for legitimate applications to 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 the operation at hand. This would require a substantial change in culture across the whole of the application provider community.

43. A third approach is to take many safety decisions away from the user altogether. Under such an approach, devices would be pre-configured with standard user profiles that restrict the purposes for which the smart device could be used. It is possible to imagine that this might work for smart devices used by minors (e.g. specific profiles for children below the age of 10, children 11 to 14, youngsters 15 to 17). However, it is less easy to see how this would work where the user of the smart device is the responsible adult. Some people will fight against the restrictions implicit in such a policy configuration. Even though these people might know that they do not understand the full implications of the changes they are making, they will override profile restrictions thereby reducing the resilience or trustworthiness of their smart device. Again, it is the attitude of the user that limits the benefit this approach can achieve. Pre-configured profiles can be part of the required response but would need to be accompanied by additional efforts to address the 'anti-security' perceptions and attitudes some people hold.

44. A fourth approach is to make users liable not only for the harm they expose themselves to through the insecurity or untrustworthiness of their devices but also for the harm they expose others to. For example, users who have allowed their PCs to be conscripted into a botnet could be made liable for the digital harm others are caused by the phishing spam their PC sends out. However, as evidenced by current efforts to hold individual serial copyright violators accountable for their actions, this type of approach is likely to be met with strong resistance from some users and some legislators.

45. Interestingly, one defence that has been used to counter enforcing liability against a user is that the user cannot be held accountable for actions performed by their PC if there is a chance that the PC might have been functioning autonomously and unbeknownst to the user as a result of its having been compromised by malware. Hence, before users can be made to carry liability for allowing their smart devices to remain insecure, smart devices would need to be made highly resilient to prevailing threats and would have to incorporate some means of warning the user when their device had been compromised by an attack. Only then could users who failed to respond be held accountable for the subsequent harm their smart device caused to others.

46. A fifth approach is to increase the inconvenience a user suffers from having a vulnerable or compromised device. Perhaps, where the potential for the user to be harmed as a result of having a compromised device has not been sufficient to induce a change in behaviour, an increase in the potential for the user to be inconvenienced might succeed. This inconvenience could take the form of application service providers issuing warnings to users whose machines appeared to have been compromised and blocking or restricting the user's access to services.

47. For this approach to work, service providers would need to accept responsibility for protecting users generally, not just for protecting their own paying customers. Some service providers follow this type of approach already. For example, some service providers will blacklist a user's IP address if the user is suspected of being a source of spam. However, many other service providers take a different attitude and do not follow this approach. Many ISPs do not disconnect servers even though they have been made aware those servers are sources of malicious code, and many e-mail service providers do not delete the malicious spam sent out by their otherwise normally behaved users. It might be that these service providers do not believe it would be right for them to take such actions or they are not inclined to follow such an approach unless they can see a business benefit arising directly from it.

48. This attitude is also reflected in the position adopted by some service providers that they are "mere conduits" of user data. According to this position, service providers have no accountability, or liability, to any users for the attacks they deliver through their infrastructures even after they have been made aware of those attacks. Such service providers are unlikely to accept any responsibility for protecting users generally unless they are made to carry some form of liability for the harm their services enable. A responsibility to users generally would normally take the form of regulation or legislation, and a liability to users generally would take the form of a fine or other penalty for non-compliance. This form would align with the way data protection legislation and non-compliance fines impose a responsibility and liability on data processors to protect the privacy of the people whose personal data they hold and process.

49. Each of the above approaches can be expected to have some beneficial effect on the behaviours of some users. No one approach is likely to be sufficient on its own to achieve a significant improvement in behaviours across a major proportion of users. That would probably require a broad multithreaded approach that brings together all of the above suggestions and includes various other steps that would be needed to address the shortcomings identified. These other steps could include efforts to address people's 'anti-security' perceptions and attitudes, means by which users could be informed when their devices have been compromised, and legislation to make service providers and users each liable for the harms they cause or enable.

Market demand for security resilient products

50. As the potential for users to be caused harm grows, consumers might start to make security resilience a buying requirement for the smart devices they purchase. This would create a demand for manufacturers to

provide more security resilience and introduce other security features into their products, and lead to people switching over to the more resilient and capable of the brands available to them.

51. However, the level of user harm experienced might need to become considerable before the forces of supply and demand on their own would generate a mass-market response to such a demand. There are two reasons for this.

52. Firstly, even if the potential for personal harm becomes considerable, people will often allow other features to take precedence over security resilience when they make their purchasing decisions. The parallel subject of car safety is illustrative. For many years, safety was one of a number of selling features in the automobile market. Many automobile brands remained successful without having equivalent safety features to the safest brands. This remained the case despite the fact that the harm people were being caused by their car's lack of safety was very considerable (up to and including death). The potential harm that people can be caused by a lack of security resilience in smart devices is usually far below that. Also, digital harms are often compensatable whereas loss of life or limb is not. This would indicate that the market for more secure smart devices might remain a niche market for a long time unless the potential harm that people can be caused by poor security becomes very much higher than it currently is.

53. Secondly, the tightness of the margins available to product manufacturers, at least within the current PC industry if not also within the mobile handsets industry, suggests that consumer demand for more secure products might have to become considerable before manufacturers would have the confidence to invest in developing product responses to that demand.

54. However, brand loyalty in the smart electronic consumer devices marketplace does not appear to be as strong as in the automobile industry. Also, the time interval between successive consumer smart device purchases tends to be less than that between successive automobile purchases. These suggest that the smart device industry might respond to emerging consumer demand more rapidly than otherwise despite the tightness of their margins, especially in those areas of the market where the margins are not yet at their tightest.

55. There are also a number of other market forces besides straightforward supply and demand that can influence manufacturers' responses.

- Consumer groups can influence market developments by giving voice to a consumer interest that would otherwise remain unarticulated. Consumer groups could arise around interests such as personal privacy or child safety.

- The government can provide consumer incentives where market forces are otherwise not sufficient. This approach has been used in other areas, for example with hybrid cars, where market forces did not prove sufficient on their own to kick start a socially desired change in consumer behaviours. The government might wish to consider if there are ways it can provide incentives to encourage consumers to take on more trustworthy and security resilient devices.

- Insurance is another force for change in the market. There is an interesting analogy with how insurers facilitated the adoption of car immobilisers at a time when increasing numbers of cars were being stolen. Information was put into the public domain about which cars were being stolen most easily or often. This led to the development of technical solutions (immobilisers) but not immediately to a large uptake of that solution by consumers. The uptake increased when insurers started pricing the presence or absence of an immobiliser into the cost of the car's insurance premium. In this way, the market worked to get the consumer to bear the cost of the lack of theft resilience of their car. This cost served as a counterweight to the cost attached to the immobiliser option on the consumer's car purchase. It is unclear how much of a role insurance will have in the smart devices arena but, where it has a role, it might be able to make the consumer bear the cost of device insecurity and encourage consumers to demand more resilient devices.

56. The more smart device manufacturers raise the security and trustworthiness of their devices, the more scope application software developers, web site developers and application service providers will have to

develop more secure and trustworthy applications and web sites. Having secure and trustworthy smart devices is a prerequisite for developers to be able to provide secure and trustworthy applications and application services. Thus the lead has to come from the device manufacturers rather than from other parties within the smart devices industry.

57. As the market starts to provide more trustworthy applications and application services, the consumer will look for ways to distinguish between those that are trustworthy and those that aren't. One response to this need could be the development of a 'kite mark' or equivalent process under which applications and application-based services would be certified against a recognised standard.

58. For a kite mark to be meaningful to the consumer, it would have to be persistent, i.e. to cover the whole lifecycle of the consumer's use of the software, web site or service. This means that the kite mark would have to cover the target's security management processes, not just the security resilience of the end product. This is particularly the case for web sites as web sites tend to be more dynamic than application software or services.

59. Building on the approach taken by the Wholesale Application Community, the smart devices industry could develop libraries of signed applications that have been granted a kite mark (and hence can be presumed by the consumer to be trustworthy and security resilient).

Users seeking redress, and the introduction of legislation

60. If the market is slow to respond to the rising levels of harm users are caused, the public's attitude to suppliers' responsibilities could start to change. People might feel that product and service providers have a duty to provide products and services that are fit for purpose and that providers should be made liable for the harm caused to people by products or services that fall short. If current consumer protection legislation did not enable manufacturers to be made liable for their products not being fit for purpose, then pressure could arise for the introduction of suitable legislative amendments.

61. Under current arrangements, smart device manufacturers do not have a duty to provide devices that are fit for any particular consumer purpose. It is common for product terms of sale to exclude any warranty that the smart device is fit for any particular purpose, and for software and web site user licences to exclude any trustworthiness or security warranties.

62. This would appear to be somewhat at odds with the arrangements that apply to many other types of consumer goods and services. In many other situations, a consumer can expect that the product or offering will be fit for the expected purpose and that the provider would make good any loss to the consumer if their product or service fell short. Retailers are required to take back or replace goods purchased in their stores that do not meet the consumer's reasonable capability or performance expectations, service providers are required to provide compensation for extended service outages, and financial service providers are required to provide refunds if account transactions are made that the account holder did not authorise.

63. This would also appear to be at odds with the fact that, in the present day digital society, people use, and are encouraged on all sides to use, smart devices for significant aspects of their personal lives. Twenty or so years ago people typically used smart devices for relatively unimportant off-line activities such as playing games, entertainment, and writing correspondence that they would then print out and post. This is no longer the case. People use smart devices, including the applications that run on them and the services they access through them, for significant aspects of their lives. These include building relationships, conducting their financial affairs and interacting with public sector services. This is actively encouraged by the UK Government through initiatives such as Digital Britain, the Digital Inclusion Task Force and the digitalisation of front-line services. Given that this is the present day situation, consumers should be able to have a reasonable expectation that the smart devices they buy or use will be fit for the purposes they can be expected to use them for. Being fit for purpose should include having an adequate level of security resilience, trustworthiness and safety, not just being adequately fast and reliable.

64. Consumer protection legislation (e.g. The Sale of Goods Act 1979 as amended) enforces the public's reasonable expectations regarding the suitability for purpose of consumer products and services. For example, the legislation requires the retailer to replace, repair or refund any product that is faulty, not fit for purpose, or that fails within the period that the consumer should reasonably be able to expect the product to work for. This requirement on retailers holds even if the terms of sale of the product provide warranty cover that is more narrowly defined or for a shorter period than it is reasonable for the consumer to expect. The public expectation of the period for which a product should work overrules the warranty period in the product's terms of sale if that warranty period is shorter. If this legislative principle were to be applied to smart devices, consumer protection legislation could be used (amended if necessary) to support this public attitude if it emerges. Product and service providers could be held to have a duty to provide products and services that are fit for consumers' present day digital society purposes, and providers could be held liable for any harm caused to users should a product or service fall short.

65. The situation with smart devices is complicated, but only slightly, by the fact that the smart device is only a platform on which the user is able to install and operate applications provided by independent application providers. No one organisation is responsible for the finished product that the consumer uses. Hence, any move to create an obligation on providers to provide smart devices that were fit for the consumer's expected purposes would have to distinguish between the device manufacturer's obligation to provide fit for purpose platforms and the application provider's obligations to provide fit for purpose applications.

66. This approach to supplier responsibilities could be extended to cover the providers of web sites and application services. Currently, anyone is permitted to build a web site without being required to take on any liability for the safety of the consumers who visit their site. Whereas a physical retailer cannot avoid public liability (and is required to take out public liability insurance) should a member of the public be harmed whilst in their store, web site providers can, and often do, explicitly decline within their terms of use any public liability should a member of the public get harmed (e.g. their smart device gets compromised by malware) while visiting their site.