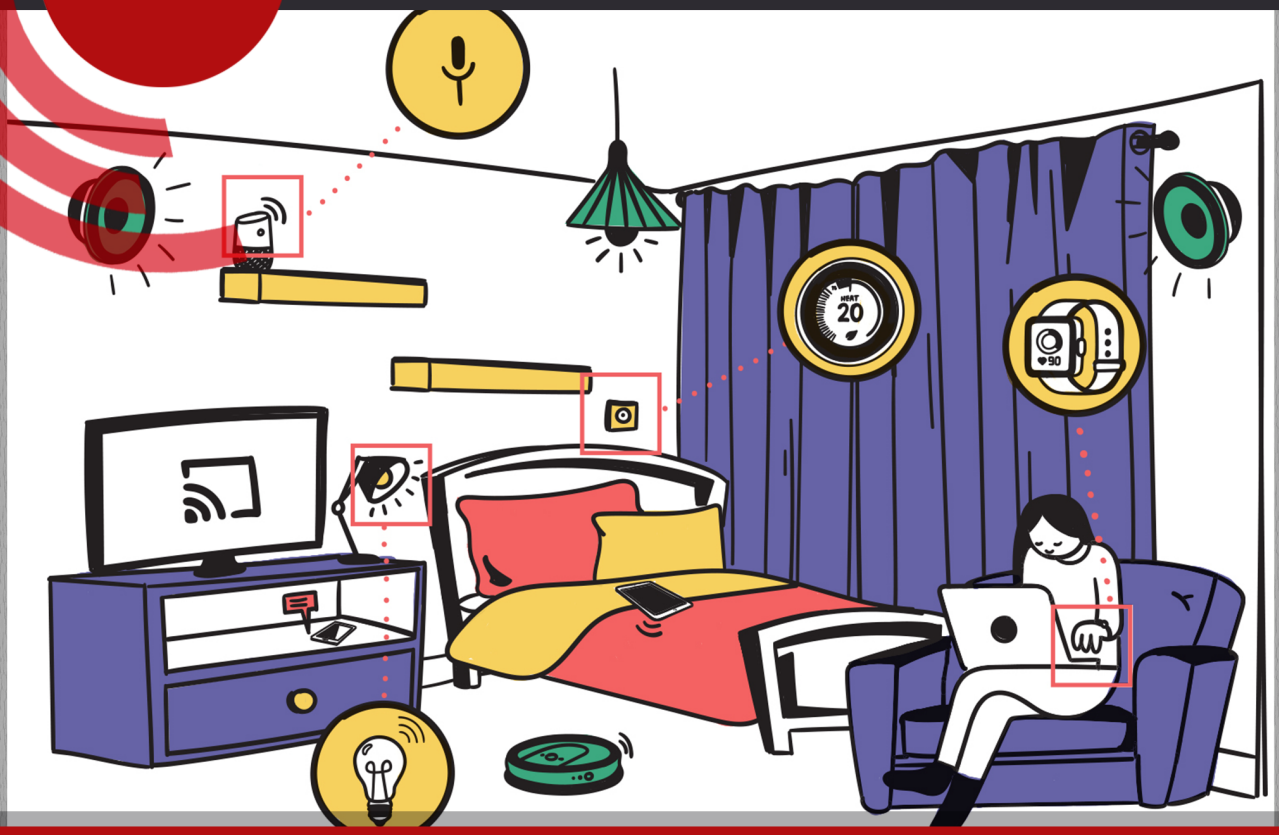
CREST Centre for Research and Evidence on Security Threats



Individual Differences in the Adoption, Secure Use, and Exploitation of Smart Home Technology

FULL REPORT

FEBRUARY 2021

Emma Williams, Emma Slade, Duncan Hodges, Phil Morgan, Dylan Jones, Bill Macken, Emily Collins and Tasos Spiliotopoulos

FEBRUARY 2021

Individual Differences in the Adoption, Secure Use, and Exploitation of Smart Home Technology

FULL REPORT

Emma Williams, University of Bristol
Emma Slade, University of Bristol
Duncan Hodges, Cranfield University
Phil Morgan, Cardiff University
Dylan Jones, Cardiff University
Bill Macken, Cardiff University
Emily Collins, University of Bath
Tasos Spiliotopoulos, Cardiff University

This research was funded by the Centre for Research and Evidence on Security Threats – an independent Centre commissioned by the Economic and Social Research Council (ESRC Award: ES/N009614/1) and which is funded in part by the UK security and intelligence agencies and Home Office.

www.crestresearch.ac.uk

UKRI Economic and Social Research Council

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report details the key findings of work conducted by the *Individual Differences in Adoption, Secure Use, and Exploitation of Smart Home Technology* project. This one-year project was commissioned by the Centre for Research and Evidence on Security Threats (CREST) in September 2019 and led by the University of Bristol in collaboration with Cardiff University and Cranfield University.

The overall project consists of three primary work packages (WPs) using smart home-based IoT technology to explore the relationship between individual differences in the adoption and secure use of new technology, and the exploitation of such technologies for nefarious purposes. The project was delivered by a multi-disciplinary team, which included experts in consumer behaviour and technology adoption, psychology and human factors in the cyber domain, and cyberspace operations.

This report provides a high-level overview of activity conducted across the three WPs:

- WP1 reviewed current literature to develop a framework for *modelling the cyber-enablement of traditional crimes through the introduction of pervasive smart home-based IoT technology*, using residential burglary as a case example.
- WP2 then deployed an online survey, collecting qualitative and quantitative data from 633 participants, to explore the relationship between *individual differences and consumer adoption, and secure use, of some of the different types of smart home technology* identified in WP1.
- Within WP3, an online experimental task was then designed and programmed to examine how *priming people regarding security and privacy may influence their decision-making in smart home contexts,* using trigger action rules as a way to explore this. Two online experiments (n = 375) were conducted to measure security and privacy settings under a range of conditions, including when participants were explicitly primed (experiment 1) and when they were implicitly primed (experiment 2) to think and act either more securely or more privately.

The approach of the latter two work packages provided a means to further consider the potential exploitation of connected smart home devices via vulnerabilities that may emerge as a result of people's choices. Recommendations arising from this work are provided, with a particular focus on how the secure adoption and use of products and services by all consumers can be facilitated, including potential integration into the product development lifecycle.

KEY POINTS

Our work shows how the opinions that people hold about technology can carry over to the choices that they make when setting up that technology. Consumers may benefit from increased engagement and education in the early stage of product consideration and use (e.g. during marketing, sales, and initial set-up/registration stages) regarding the relevance and importance of security for different types of smart home devices, particularly those not traditionally viewed as relevant to security. For current users of devices, engagement via existing customer relationship management channels may provide a useful route (e.g. Dewnarain, Ramkissoon & Mavondo, 2019). More generally, this research suggests the importance of stressing the dangers to security and privacy from being overly trusting of technology and its applications, as well as highlighting the risks of particular types of use.

As part of these communications, current adopters and non-adopters of smart home technology would benefit from targeted communications differentially focused

on emphasising potential risks and benefits (e.g. Key & Czaplewski, 2017). This would enable current adopters to better understand (and mitigate) security risks and non-adopters to understand the potential benefits that smart home technology may bring to their lives.

A balanced view of security risks should be encouraged via end-to-end collaboration internally within organisations, with security, product development, and consumer behaviour and marketing professionals all actively engaged to consider the full product lifecycle – from product development to adoption and eventual discontinuance (e.g. Jugend, Ribeiro de Araujo, Pimenta, Gobbo & Hilletofth, 2017). To ensure sufficient understanding and buy-in across these groups of the needs and priorities of the other, internal marketing mechanisms may provide a useful structure to communicate and develop a shared internal vision of secure, consumer-focused innovation in relation to smart home devices, which can then be effectively communicated to consumers (e.g. Ballantyne, 2003; Kadic-Maglajlic, Boso & Micevski, 2018).

Increasing consumers' perceived proficiency with technology, both directly related to security aspects and wider technology interactions, may facilitate greater confidence to both adopt such technologies and to use them securely. Our work also suggests that people could benefit from more support in understanding how their systems are configured and the likely knock-on effects of upgrades and additions. The use of community-focused, grassroots networks and organisations to develop and support technology proficiency within the community may increase the likelihood that such approaches can target a diverse range of consumer groups (e.g. Nicholson, Coventry & Briggs, 2019). Explicitly linking such approaches with existing, trusted organisations (e.g. across NGOs, industry, and the public sector) via sponsorship or other activities, may provide further credibility to networks and community technology support spaces, both in offline and online environments. Such approaches should provide support across the product lifecycle.

Reducing perceived vulnerability arising from using technology may increase the adoption of smart home technology but may also contribute to more insecure behaviour as a result if not managed appropriately. An approach that focuses on helping consumers to feel able to effectively manage any potential vulnerabilities that emerge rather than simply influencing perceptions of threat is likely to be preferable, and will also assist in building consumer resilience to emerging security risks as technology develops (e.g. Brass & Sowell, 2020; van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019). Such an approach will likely require flexible and adaptive engagement with the community, or other trusted and accessible, support mechanisms. Such approaches should provide support across the product lifecycle.

Although risk information may increase secure behaviour it may also reduce intentions to use such devices. Therefore, exposure to media information regarding the risks of smart home technologies should be accompanied by protective information that educates consumers on how they can easily manage these to increase secure behaviour without reducing usage or adoption of devices. Such information would likely benefit from the responsive, coordinated, and adaptive approaches typically seen in effective online crisis communications (e.g. Roshan, Warren & Carr, 2016).

Privacy and security work in slightly different ways and this requires more investigation. In the current work, although explicitly priming people to focus on improved security behaviours, it appeared to have an adverse impact on privacy behaviours. On the other hand, implicitly priming people to focus on privacy behaviours was shown to improve both privacy and security behaviours. As such, interventions in the smart home context should be carefully considered regarding the particular behaviour that they are aiming to encourage and the wider impacts that they may have on related behaviours.

PROJECT BACKGROUND

The advent of the Internet of Things (IoT) has raised the prospect of increasingly connected devices within the home, with new technology that has traditionally been standalone now being able to connect to the Internet and other devices. The global market for IoT technology was worth an estimated 194.5 billion US dollars in 2017 (Statista, 2018a), and it is predicted that the number of households with smart devices in the UK will rise from 8.4% in 2017 to 26.8 % in 2022 (Statista, 2018b).

From smart locks and home surveillance systems to connected appliances, light bulbs, and heating systems, such technology presents multiple advantages for saving energy, time and money, providing increased convenience and flexibility within daily life (Sovacool & Furszyfer Del Rio, 2020; Wilson, Hargreaves & Hauxwell-Baldwin, 2017). However, such technology also presents risks, not only to data security but also to personal safety (e.g. Blythe & Johnson, 2019). This is due to the potential exploitation of such devices in facilitating 'traditional' forms of crime, such as burglary, extortion, harassment, and abuse (e.g. Heartfield, Loukas, Budimir, Bezemskij, Fontaine, Filippoupolitis & Roesch, 2018). To maximise the benefits that digital innovation, such as smart home technologies, can bring to society, it is vital to understand the factors that may influence their adoption and use, and how these may contribute to (or mitigate against) potential security risks.

Although work in consumer behaviour and innovation has highlighted a range of different factors that may influence technology adoption more generally (e.g. Agarwal & Prasad, 2007; de Boer, van Deursen & van Rompay, 2019; Featherman & Pavlou, 2003; Kim & Shin, 2015; Lin, Shih, & Sher, 2007; Mani & Chouk, 2018; Nikou, 2019; Park, Kim & Jeong, 2018; Ratchford & Barnhart, 2012; Wilson et al, 2017; Wünderlich, Wangenheim & Bitner, 2013; Yang, Lee & Zo, 2017), the need for more consumer-focused research across a broad range of consumer groups is increasingly recognised, both in relation to what influences initial adoption of smart home technologies and how such devices are used within the home (Coughlin, D'Ambrosio, Reimer & Pratt, 2007; Marikyan, Papagiannidis & Alamanos, 2019; Sovacool & Furszyfer Del Rio, 2020).

The importance of user behaviour in influencing the cybersecurity of technologies is well-known (e.g. Beautement, Sasse & Wonham, 2008; Das, Kim, Jelen, Streiff, Camp & Huber, 2020; Hadlington & Chivers, 2018; van Shaik, Jansen, Onibokun, Camp & Kusev, 2018; van Schaik, Jeske, Onibokun, Coventry, Jansen & Kusev, 2017; Williams, Hinds & Joinson, 2018). Consumer consideration of security when purchasing, setting up, and managing their devices in the home environment can all help to reduce the security risks of smart home technology (NCSC, 2019). However, it is currently unclear how differences in the adoption and secure use of smart home technology by different consumer groups may influence the potential for emergent vulnerabilities, and what can be done to reduce this. For instance, to what extent are different users likely to consider, understand, and mitigate potential security and personal safety risks associated with the technology that they purchase? This is particularly relevant since many smart products, such as smart fridges and TVs, are items that have not traditionally been associated with posing a security risk (e.g. Hubert, Blut, Brock, Zhang, Koch & Riedl, 2019; Shin, Park & Lee, 2018).

The reported project aimed to address this knowledge gap, focusing on smart home technology and cyber-enabled crime (where a traditional crime can be simplified or amplified as a result of device vulnerability; McGuire & Dowling, 2013) as a basis to explore the relationship between individual differences

in the adoption and use of new technology, and the exploitation of such technologies for nefarious purposes.

Specifically, the project set out to:

1. Use home-based IoT technology as a framework to identify the potential of these devices to be exploited for criminal purposes via the 'cyber-enablement' of particular crimes, with a focus on residential burglary as a case example.
2. Investigate the influence of individual differences in psychological characteristics, such as risk propensity, impulsivity, and technology adoption propensity, and socio-demographic factors, such as age, gender, and education, on the adoption and secure use of these devices at the consumer level.
3. Consider how these individual differences and other factors (including the extent to which people are encouraged to prioritise security and privacy issues) link to the use of IoT devices and as such influence the emergence of vulnerabilities that could be exploited by nefarious individuals.

To achieve these objectives, the project involved a multi-disciplinary team across three research-intensive UK universities (School of Management at the University of Bristol, School of Psychology at Cardiff University, and Centre for Electronic Warfare, Information and Cyber at Cranfield University). This allowed the project to benefit from expertise in consumer behaviour, marketing and technology adoption, psychology and human factors in the cyber domain, and cybersecurity.

A mixed-methods approach was used across the project, encompassing:

1. An initial review of open-source materials to identify and map smart home-based IoT vulnerabilities, using residential burglary as a case example, and the development of a methodology for application to other forms of crime (WP1).
2. A large-scale online survey capturing both quantitative and qualitative data to explore individual differences in the adoption and secure use of smart home technology, with secure behaviour scenarios developed, and particular device types used, based upon the vulnerability mapping exercise developed in WP1 (WP2).
3. Experimental work to explore the influence of specific factors (namely, human consideration of security and privacy settings (e.g. trigger action rules, IFTTT) of smart home devices) on the secure use, and potential exploitation, of these technologies within smart home contexts (WP3).

The remainder of this report provides a high-level overview of each area of work, alongside key findings and outputs.

MAPPING SMART HOME-BASED IOT VULNERABILITIES

Residential burglary can be defined as a traditional crime occurring in a predominantly offline environment. However, as smart home technology becomes more prevalent, our homes can no longer be considered to be purely offline spaces, but are instead becoming complex cyber-physical systems. Given this shift, it is important that academics and practitioners alike begin to consider the potential for traditionally offline crimes, such as burglary, to become 'cyber-enabled'. Put simply, this means that such crimes can be simplified, or increased in their scale or reach, by the use of computers, computer networks, or other forms of information communication technology (ICT).

Historically, cyber-enabled crimes have been considered to be those crimes associated with activities such as fraud and data-theft– this is perhaps not surprising given the informational assets associated with such activities. However, as our homes increasingly include some form of domestic smart technology, we begin to allow this ICT to physically interact with the offline space of the residential property (whether to turn on lights, change the temperature, or grant entry to the property), thus offering the opportunity for cyber-enablement of crime in such contexts.

Academia has invested a significant amount of time and effort to better understand the cyber risk associated with smart homes (e.g. Ali & Awad, 2018; Bashir & Mir, 2018; Blythe & Johnson, 2019). There are many frameworks for understanding potential 'harms' and the theoretical risk from an increase in the risk of information disclosures. The focus of this work package was to provide an improved contextualisation of this cyber risk within the significant body of literature associated with more traditional forms of crime.

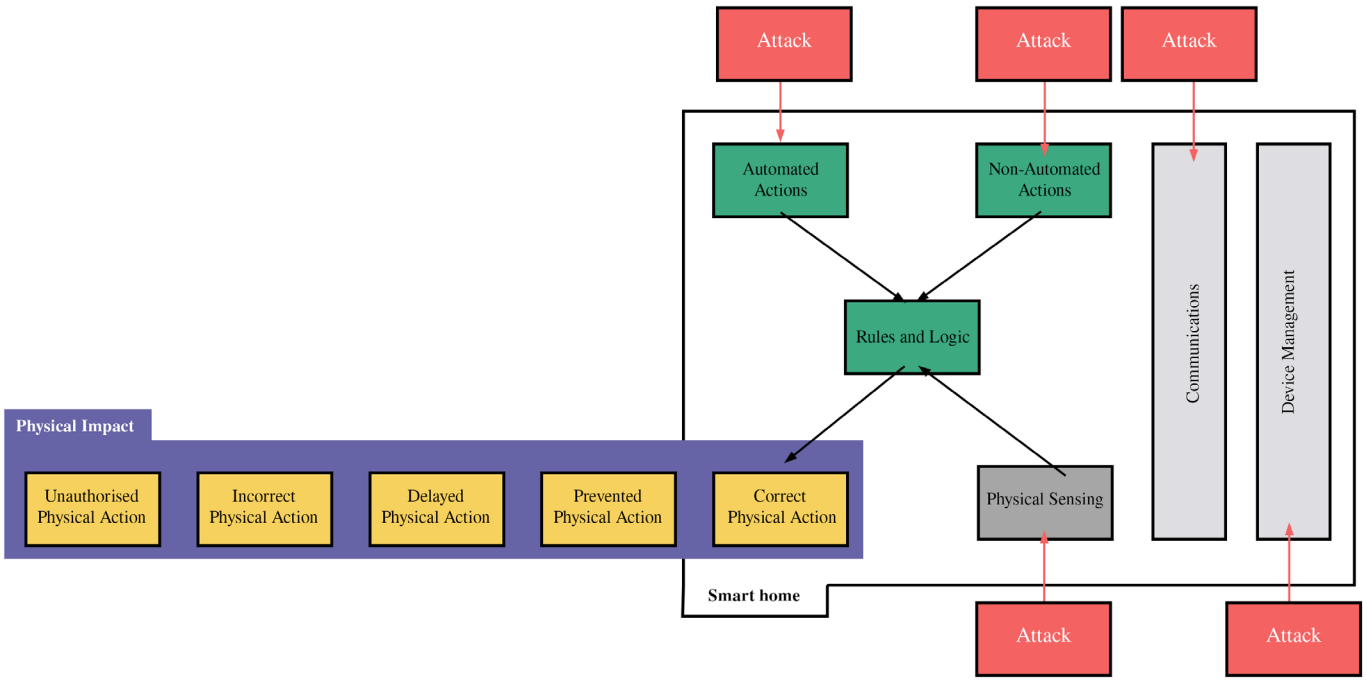


Figure 1: Primary malicious physical impacts that may arise following a successful attack on a smart home.

A thorough review of the relevant models for understanding the cyber-physical risk associated with the smart home was undertaken, with common elements from multiple models synthesised to provide a high-level understanding of the cyber-physical risk associated with a smart home. It is noteworthy that this is a relatively simple model at a high-level of abstraction with the assumption that any successful attack could result in one of the four malicious physical outcomes shown in *Figure 1.*

The above abstraction allowed us to simply consider the four physical impacts within the context of criminal activity. A structured review of the main features of smart homes then allowed us to identify a number of representative smart home deployments. The first of these was a 'simple' smart home with relatively 'passive' one-way control, the second was a 'complex' smart home, which adds elements of feedback and a richer understanding of the environment surrounding devices, and the third and final smart home was a 'complete' smart home, which is designed to represent the majority of devices currently available on the UK

Simple		Complex		Complete	
Hub	A smart hub (e.g. Amazon Alexa, Google Home)	Hub	A smart hub (e.g. Amazon Alexa, Google Home)	Hub	A smart hub (e.g. Amazon Alexa, Google Home)
Lights / socket	One or more smart light bulbs or plug sockets	Lights / socket	One or more smart light bulbs or plug sockets	Lights / socket	One or more smart light bulbs or plug sockets
Speaker / TV	Either a smart TV or smart speakers – this may be integrated into hub device	Speaker / TV	Either a smart TV or smart speakers – this may be integrated into hub device	Speaker / TV	Either a smart TV or smart speakers – this may be integrated into hub device
		Thermostat	The ability to control the temperature of the space	Thermostat	The ability to control the temperature of the space
		Camera	A dedicated security camera or security solution	Camera	A dedicated security camera or security solution
		Doorbell	A smart doorbell providing a video link from the door and a two-way audio link	Doorbell	A smart doorbell providing a video link from the door and a two-way audio link
				Lock	A lock opened by a smartphone device, with the possibility to delegate access to other devices
				White Goods	Fridge, freezers, and washing machines which allow either simple control or notifications via smartphones / web apps or hubs.
				Vacuum Cleaner	Self-propelled and automated vacuum devices

Table 1: Overview of the three representative smart home deployments.

high-street or via mainstream online retailers. These various smart home deployments are visualised in *Table 1*.

With this structured understanding of both the malicious effects that are achievable in a smart home context and the potential composition of smart homes in the current consumer environment, the final step is to apply this to a structured understanding of how residential burglary is committed. Residential burglary involves a complex decision-making process that cannot be simply divided into planned and spontaneous burglary. Using the academic literature surrounding residential burglary, we can build a structured understanding of an experienced burglar's decision-making process. This decision-making process is depicted in *Figure 2*.

Using these three frameworks (i.e. the understanding of the malicious physical impact that can be achieved through a cyber-exploitation of the smart home, the constituents of the smart home itself, and the understanding of how residential burglary is committed) it is possible to identify the interaction between these and the potential for cyber-enablement of this form of crime within smart home contexts.

KEY FINDINGS

In general, there is little or no impact from the smart home on residential burglary. With current approaches to residential burglary, it is unlikely that the adoption of smart home devices will substantially affect the risk of residential burglary. However, there may be increases in other risks associated with other activities – for example, an increase in privacy concerns.

From our analysis, one of the elements of the smart home that did appear to increase the risk of residential burglary were external devices, such as smart doorbells. These are a very visible, external part of the smart home and provide a very salient relative-affluence cue indicating that the resident is likely to be relatively wealthy. Although these devices often support video capability, it is rare for a burglar to enter through the front of a property where this video recording capability is likely to focus.

One of the key elements when considering residential burglary that may be enabled by the smart home is smart locks since these represent a device that can provide direct access to the property. Smart locks are still a relatively rare device to be present on a property and, as such, even an experienced and prolific burglar is likely to rarely encounter these devices. From the academic literature surrounding residential burglary, one of the key themes is the burglar's desire to maximise their familiarity with the property, so there may be a small deterrent effect due to the relative obscurity of these devices. However, as discussed previously, it is also relatively rare to break into the property through the front door.

Burglary that looks to exploit information disclosures through cyberspace to support a variety of the cues shown in *Figure 2* is unlikely to present a major threat in the short- to medium-term. This information-centric approach to residential burglary will suffer from challenges associated with linking a disclosure in the cyber domain to a precise physical location. It will also suffer from the fact that to commit residential burglary, there is a requirement to be physically present at a given location, so there is little immediate benefit to identifying these cues at a greater distance. It is also noteworthy that there are existing technologies (e.g. Google Street View) that research has shown can be used to identify relevant affluence and layout cues, yet there is little evidence of the widespread use of such tools within current residential burglary.

If we consider the likely path to more prevalent exploitation of smart home technology for residential burglary, there are several potential future indicators. The first of these is likely to be an increase in IoT exploitation during commercial burglary. The burglary of commercial premises tends to be a more planned undertaking, and planned undertakings are more likely to exploit information disclosures, particularly prior

to arriving at the location. The second indicator is the potential increase in the use of marketplaces that supports those experienced burglars; we have already seen cyber-criminals working together to exploit each other's different skill sets while enabling and indeed rewarding specialism. There is the potential in this case for similar co-operation between those proficient in online and off-line criminal activity, and although there will likely be challenges and potential friction between these two communities, the opportunities, particularly for high-value, planned burglary targets, may be sufficient to overcome these.

While at present the opportunity for a cyber-enabled burglary exists, in the future criminals who are motivated and capable to exploit this opportunity may also exist and hence the extent of future adoption of such devices by consumers and the relative ease with which they can be exploited by others are likely to be crucial factors.

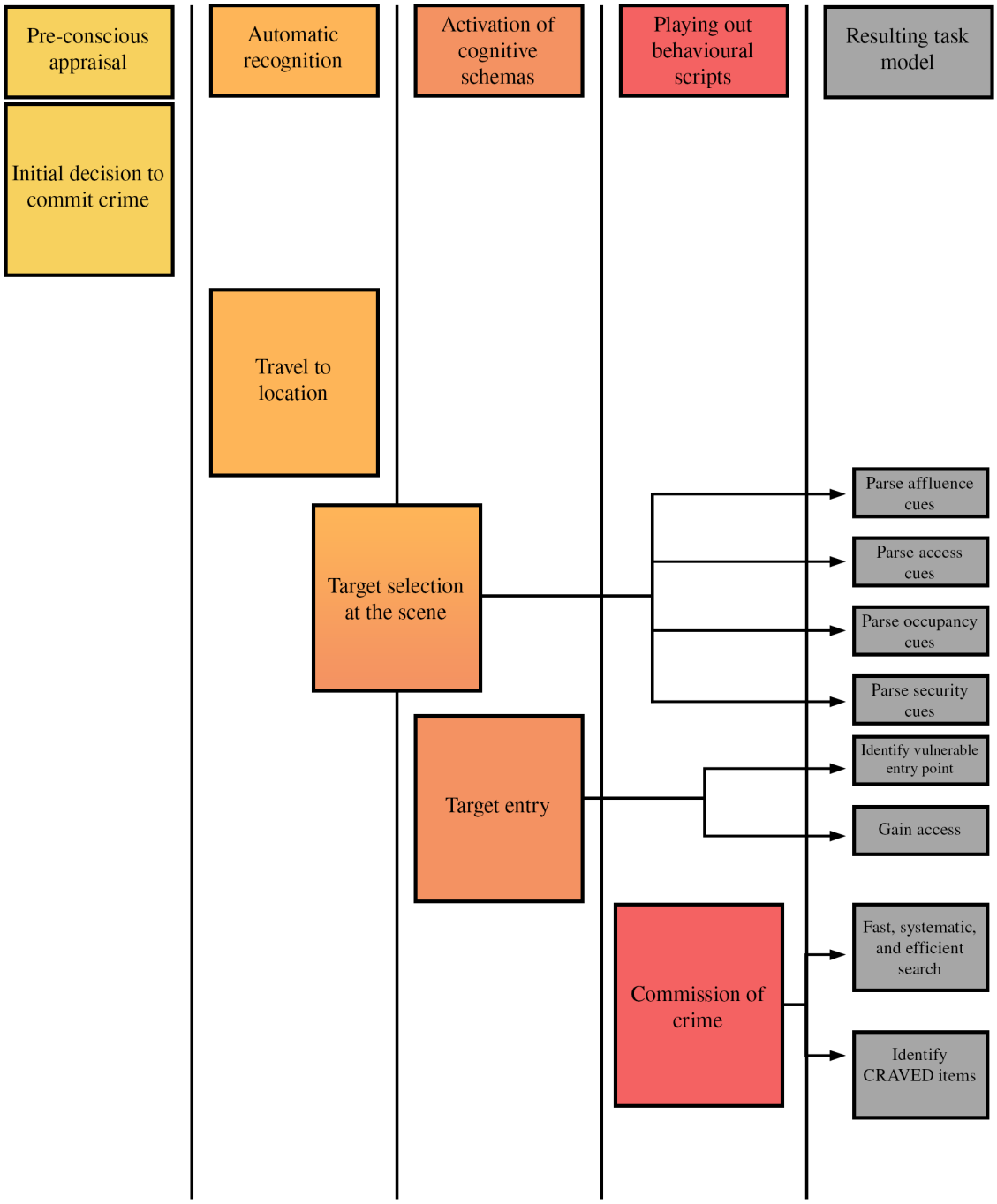


Figure 2: Depiction of an experienced burglar's decision-making process.

INDIVIDUAL DIFFERENCES IN ADOPTION AND SECURE USE OF SMART HOME TECHNOLOGY

WP2 investigated individual differences in consumer behaviour related to the adoption and secure use of smart home-based technologies, considering how, through their behaviour, different consumers may make such technologies more or less vulnerable to exploitation by criminals. An online survey approach was used, combining previous technology adoption and consumer behaviour literature (e.g. Agarwal & Prasad, 2007; de Boer et al, 2019; Featherman & Pavlou, 2003; Kim & Shin, 2015; Lin et al, 2007; Mani & Chouk, 2018; Marikyan et al, 2019; Nikou, 2019; Park et al, 2018; Ratchford & Barnhart, 2012; Wünderlich et al, 2013; Yang et al, 2017) with the outputs of WP1 to provide a foundation for the work.

Security behaviour scenarios have previously been used to examine human behaviour concerning information security within workplace settings (e.g. Siponen & Vance, 2010). For the current work, four security scenarios were developed based on particular smart devices and security behaviours, aided by the vulnerability mapping undertaken in WP1.

These security scenarios related to four different touchpoints across the consumer product journey that have the potential to exacerbate, or indeed mitigate against, security vulnerabilities related to smart home technologies. These touchpoints were:

- when a consumer chooses a product
- when they first set it up in their home
- the longer-term management of the product
- the potential discontinuance of the product.

These scenarios were specifically designed to feature one of two different device types: smart locks (which are traditionally associated with physical security and allow control over physical entry to the domestic space) or smart lights (which are traditionally associated with internal domestic experience).

Participants were randomly split into two groups and responded to all four scenarios for one of the device types.

> *"Danni has just purchased a new smart light and has been going through the user manual in order to set it up. Although the manual provides a lot of information about setting up various functions and accounts, these look a bit complicated and unnecessary. Danni realises that the device has a factory default setting, which means that you do not need to change or do anything to use the device, so decides to just use this for now."*
>
> (Example scenario: Product set-up; smart light)

The online survey examined the influence of specific individual characteristics on both responses to these scenarios and self-reported adoption of smart home technology. In particular, the following individual characteristics were investigated:

- Differences in risk-taking propensity (measured using the Domain-Specific Risk-Taking scale (DOSPERT): Weber, Blais & Betz, 2002)
- Differences in impulsivity (measured using the Barratt Impulsiveness Scale (BIS): Patton, Stanford & Barratt, 1995)
- Differences in technology adoption propensity (measured using the Technology Adoption Propensity Index: Ratchford & Barnhart, 2012)

- Differences in socio-demographic factors (e.g. age, gender, educational level)

The influence of external aspects on adoption and secure use was also explored, including device type (e.g. Hubert et al, 2019; Shin et al, 2018) and information about smart home vulnerabilities communicated in the mainstream media (e.g. BBC News, 2018; Wahlberg & Sjoberg, 2000; Williams & Joinson, 2020).

Since we were also interested in people's wider views regarding what would influence them to adopt smart home devices and their related security behaviour for each of the scenario descriptions, the questionnaire also included open-ended questions to enable us to collect and analyse qualitative data related to this.

KEY FINDINGS

Overall, 633 UK-based participants across a range of ages (18–79 years; average age = 40 years) and backgrounds completed the survey between December 2019 and January 2020 via the *Prolific online participant recruitment panel*.

Quantitative data were analysed using a variety of correlational and comparative statistical approaches. For adoption of smart home devices, primary findings suggested that those who were more optimistic about technology, those who considered themselves more proficient in using technology, and those who felt less vulnerable concerning technology use, were more likely to use smart home technologies.

Qualitative data relating to what would most influence people to use smart home technology suggested that many people have security concerns related to the use of such technology, but that the key question was whether the potential benefits were considered to outweigh these potential risks – and different people had very different views on these aspects.

For our security scenarios, primary findings from our quantitative data suggested that both feeling more vulnerable from technology use and considering oneself more proficient in using technology was related to more secure behaviour. This highlights the potentially complex role of both perceived ability to manage technology and perceived vulnerability to security threats in both the adoption and secure use of smart home devices.

Participants also showed more secure behaviour concerning the smart lock devices than the smart light devices, suggesting that security actions are more likely to be prioritised for those products that are traditionally associated with security and protecting the physical space of the home. Interestingly, for both product types, secure behaviour appeared to generally be greater in the initial interactions with the device (e.g. during product choice and initial set-up) compared to the later stages (e.g. longer-term device management and product discontinuance). This may be due to reduced focus on, and less attention given to, devices that one has had for a longer period of time. Alternatively, it may be that people have less awareness of potential security threats related to these time points.

Qualitative data related to scenario responses was also captured in the form of asking participants to elaborate on their numerical responses to each of these scenarios. This highlighted the complexity of factors that are likely to influence such behaviours and the differences in approach shown across individuals.

For product choice, this included the differential influence of factors such as device type, price, functionality, brand reputation, and the relative importance of security features to the individual (including whether security by default is assumed).

For product set-up, this ranged from people who claimed to always check the settings at the time, to those who plan to amend later or are happy to rely on default assumptions.

For product maintenance, approaches varied from those who tended to assume that things were fine if the device was working, to those who reported always checking and updating settings.

Finally, for product discontinuance (whereby the device appears to no longer be working optimally or as expected), individuals differed according to whether they would put effort into investigating the cause of potential problems and try to fix it, to whether they would simply stop using it completely, or choose to ignore the problem and continue using the device for as long as possible.

Table 2 (below) provides an overview of these qualitative themes across the different scenarios.

Finally, participants reported a greater likelihood of reading guidance related to secure use after viewing a media story highlighting the risks of smart home technology. However, they also showed lower intentions to use smart home technology in the future as a result, although the extent to which this is actually reflected in a change in behaviour is unknown, nor how long any such effect may last.

Overall, findings suggest that:

- individual differences in how people view technology
- the particular device type used (i.e. where a product 'sits' within the vulnerability mapping of WP1)
- differences in security-related behaviour across the four product touchpoints are all likely to influence the relative security of devices and their resultant vulnerability to exploitation in the smart home context.

Two user personae have been developed based on the main findings of the survey related to these individual differences. These link individual characteristics to adoption and secure use behaviours. They provide an initial basis from which to consider whether different individual characteristics may influence cyber-related vulnerability in smart home contexts and identify where targeted mitigations may be beneficial to maximise secure adoption of smart home technologies across society.

Themes from Scenario 1 Product Choice	Themes from Scenario 2 Product Set-Up	Themes from Scenario 3 Product Maintenance	Themes from Scenario 4 Product Discontinuance
Role of device type	Would check or adjust	If it's working, it's fine	Would investigate issues
Relative importance of security features	Will amend later	Would still check	Would stop using
Assume security by default	Basic/default settings sufficient	Always tinkering or checking	Would keep using
Importance of other product factors			

Table 2: Qualitative themes emerging from open-ended responses to each of the security scenarios.

EXPERIMENTAL EXAMINATION OF SECURE USE AND POTENTIAL EXPLOITATION OF SMART HOME TECHNOLOGY

This part of the project involved the development and testing of a distinctive and relatively novel approach to the study of individual differences in the use of smart home devices. In particular, an experimental scenario was developed focused on people's decisions related to so-called trigger action rules. Such rules provide a means for people to connect apps and devices to create more complex cyber-physical systems within their homes, and can thus be related to the more complex iterations of a smart home identified in WP1. If This Then That (ITTT) rules represent one type of trigger action rule, which allow people to use some type of event in one app or device to trigger an output in another. For example, one such rule that may be used for smart doorbells includes 'When the camera on my smart doorbell detects an unknown or suspicious person (e.g. someone who lingers on my property for over 20 seconds), send a photograph of that person and a text message to my neighbours'.

The choices that people make about such rules can have security and privacy implications. As a result, they provide an interesting and targeted way to explore the factors that may influence people's decision-making with regards to privacy and security in smart home contexts. In this way, individual differences in the decision to use various types of rules, and the extent to which they reflect secure and privacy-preserving behaviours concerning the use of smart home devices, can be examined. This not only increases our understanding of the factors that may influence secure behaviours in smart home contexts but also of how such choices may influence the potential exploitation of smart home devices by criminals (e.g. the vulnerabilities that may emerge as a result of the particular settings chosen, etc.).

Instead of relating a range of demographic and attitudinal factors to naturally occurring behaviour, a setting was contrived in which we observed people's decision-making about security and privacy concerning a simulated domestic security system. To do this, a library of trigger-action rules was developed in which each rule was given a score reflecting the level of risk to security and privacy. Rules were created by the Cardiff University research team and aimed to build upon the findings of WP1 and WP2. They were then evaluated using a Delphi method, with independent experts assigning a security score and a privacy score to each rule.

The context in which the rules were to be deployed was then systematically varied, contrasting a neutral context with (a) one in which security was emphasised and (b) one in which privacy was emphasised. Not only did this provide a means to explore the potential effect of interventions related to these two contexts on people's decision-making, but it also allowed for consideration of how individuals may behave differently in such contexts if they have a heightened focus on security or privacy issues.

We were interested in ways in which we could improve people's security and privacy scores by priming them in different ways. Therefore, in the first experiment, explicit priming of either security or privacy was used, which involved giving participants explicit instructions to focus on one or other of these aspects. In the second experiment, implicit priming of either security or privacy was used; with participants first undertaking

an apparently unrelated activity that involved solving a security or privacy-related problem before engaging in the primary task.

In all, 375 volunteer participants undertook the experiments online (150 in experiment one, 225 in experiment two). Across the two experiments, each participant was asked to select rules that they thought best suited the particular context. This resulted in two aggregate scores based upon the different rule types, one for security and one for privacy.

Similar to WP2, the potential role of individual differences related to this rule-enabling task was also explored. A wide range of individual difference characteristics was examined via questionnaires covering a number of behaviours: the propensity to adopt technology, perceptions of security risks, trusting beliefs, and privacy concerns.

KEY FINDINGS

Overall, three trends emerged from the results.

The first is that the pattern of interaction with individual differences is context-dependent. That is, particular individual differences assume greater or lesser prominence depending on the context of the behaviour; where the context is open-ended (i.e. where people are not encouraged to focus on particular elements), abstract attitudes and beliefs about information technology are more influential, but when attention is more focused on optimising the choice of rule (for either security or privacy) the influence of these factors falls away and other factors become more important, such as those associated with education and experience with computer systems.

Individual differences related to security and privacy choices also emerged. For instance, regarding their security-specific choices, those who showed greater awareness of privacy practices of smart home companies tended to be less risky in enabling rules to connect devices and services. Conversely, those with greater concern about exercising control over personal information demonstrated lower security scores – potentially a preoccupation with having control over privacy may lead people to neglect considerations of security. However, regarding privacy-specific choices, it appears that both the more people trust online companies and the more they expect to benefit from smart home technologies, the less likely they are to keep their personal information private. First and foremost, this reinforces the importance of understanding how different consumers consider, and respond to, both security and privacy issues that correspond to their smart homes.

The second trend is that encouraging an individual to focus on security or privacy can improve decision performance; in some cases, this is specific to the decision context (i.e. whether it is a security or privacy-related decision), whereas in others this can generalise across both types of behaviour (i.e. both security and privacy are improved in certain conditions). Table 3 (below) overviews the impact of the various priming conditions on security and privacy scores. Specifically, explicit primes improve the score where it is targeted, with the security prime improving security scores and the privacy prime improving the privacy scores.

Prime	Type	Security score	Privacy score
Explicit	Security	Increase	Decrease
	Privacy	-	Increase
Implicit	Security	Increase	-
	Privacy	Increase	Increase

Table 3: Summary of findings for privacy and security-related primes and associated decision outcomes.

However, interestingly, in such conditions, the security prime also appears to result in privacy being neglected, with a reduction in privacy score, an effect that is not mirrored for the privacy prime.

Finally, the third trend is that the more direct the intervention, the more effective the outcome is likely to be. The effects of implicit priming were not strong or large, but the results do show that merely thinking in general terms about security or privacy has some effect, albeit not much.

Findings from this work can assist in the identification of potential ways in which end-user development can be supported and made less risky, as well as providing recommendations for future research. These are currently being finalised for journal submission and peer review. In addition to contributing to current understanding regarding individual differences in the secure use and potential exploitation of smart home technology, this part of the project has also produced a web-based tool that can be used to explore trigger-action behaviour more generally, including routes to the adoption of such technology, as well as to gain a more in-depth understanding of how such technology can be exploited, and thus better protected, at both the human and system level.

SUMMARY AND RECOMMENDATIONS

This one-year project has taken a multidisciplinary approach to explore the various factors that influence how people engage with smart home technologies and the exploitation of these technologies for nefarious purposes. In particular, it has focused on exploring:

1. how security vulnerabilities related to smart home technologies can be mapped and conceptualised
2. how various individual differences in the adoption and secure use of particular smart home devices are likely to contribute to such vulnerabilities, and how this can be mitigated
3. how different factors can be experimentally manipulated to influence secure use, and thus minimise the potential exploitation, of devices.

LIMITATIONS AND FUTURE WORK

This project used a range of methods to explore the adoption, secure use, and exploitation of smart home technology. However, as with all research, this work was not without limitations and future work would therefore be beneficial to address these aspects.

Firstly, to effectively bound the project within the resource and time available, the work focused on a particular case example (residential burglary) when considering potential vulnerabilities arising from smart home technologies. Although a general framework has been provided to enable this approach to be undertaken for other threat scenarios, this was not undertaken within the current project. Therefore, further work would be beneficial to test this framework methodology within other threat scenarios (e.g. domestic abuse, harassment, etc.).

Secondly, the survey work relied on participant self-reports regarding their adoption of smart home devices, security behaviour, and future intentions. As such, future work that can measure actual behaviour within domestic scenarios would be beneficial. It should also be noted that, as with the majority of marketing and psychology-based research, the survey was completely voluntary and the participant sample may thus be influenced by a degree of self-selection bias. However, to achieve as diverse a sample as possible, subgroups of participants were specifically targeted using the Prolific participant panel specified features to ensure a relatively even spread of age groups was represented (e.g. 18–30 years, 31–50 years, 51+ years; average age: 40 years; age range: 18–79 years). The participant sample was also shown to represent a range of educational and employment backgrounds. However, further work would be beneficial that targets a more diverse population (in particular, those individuals who may be less likely to engage with online surveys and online environments) and that considers consumers based outside of the UK.

Finally, for the experimental work, only two experiments were undertaken with a new task and paradigm developed specifically for this research, and so it is important not to over-generalise findings without further investigation (i.e. replication of findings and extension of work using this task and paradigm). Despite well-powered studies (n = 150 for experiment 1, n = 225 for experiment 2) for exploring the security and privacy data, a larger number of participants would be beneficial in relation to the individual difference measures, and this work is currently underway. Future work that shifts the focus of individual difference research towards creating a tool that can predict an individual's vulnerability to making inappropriate choices in such contexts may also be useful to continue to develop more targeted interventions.

KEY RECOMMENDATIONS

Based on the outcomes of this project, the following recommendations are provided regarding how the secure adoption of products and services by consumers can be facilitated, with a particular focus on potential integration into the product development lifecycle.

Our work shows how the opinions that people hold about technology can carry over to the choices that they make when setting up that technology. Consumers may benefit from increased engagement and education in the early stage of product consideration and use (e.g. during marketing, sales, and initial set-up/registration stages) regarding the relevance and importance of security for different types of IoT devices, particularly those not traditionally viewed as relevant to security. For current users of devices, engagement via existing customer relationship management channels may provide a useful route (e.g. Dewnarain, Ramkissoon & Mavondo, 2019). More generally, this research suggests the importance of stressing the dangers to security and privacy from being overly trusting of the technology and its applications, as well as in highlighting the risks of particular types of use.

As part of these communications, current adopters and non-adopters of smart home technology would benefit from targeted communications differentially focused on emphasising potential risks and benefits (e.g. Key & Czaplewski, 2017). This would enable current adopters to better understand (and mitigate) security risks and non-adopters to understand the potential benefits that smart home technology may bring to their lives.

A balanced view of security risks should be encouraged via end-to-end collaboration internally within organisations, with security, product development, and consumer behaviour and marketing professionals all actively engaged to consider the full product lifecycle – from product development to adoption and discontinuance (e.g. Jugend, Ribeiro de Araujo, Pimenta, Gobbo & Hilletofth, 2017). To ensure sufficient understanding and buy-in across these groups of the needs and priorities of the other, internal marketing mechanisms may provide a useful structure to communicate and develop a shared internal vision of secure, consumer-focused innovation in relation to smart home devices, which can then be effectively communicated to consumers (e.g. Ballantyne, 2003; Kadic-Maglajlic, Boso & Micevski, 2018).

Increasing consumers' perceived proficiency with technology, both directly related to security aspects and wider technology interactions, may facilitate greater confidence to both adopt such technologies and to use them securely. Our work also suggests that people could benefit from more support in understanding how their systems are configured and the likely knock-on effects of upgrades and additions. The use of community-focused, grassroots networks and organisations to develop and support technology proficiency within the community may increase the likelihood that such approaches can target a diverse range of consumer groups (e.g. Nicholson, Coventry & Briggs, 2019). Explicitly linking such approaches with existing, trusted organisations (e.g. across NGOs, industry, and the public sector) via sponsorship or other activities, may provide further credibility to networks and community technology support spaces, both in offline and online environments. Such approaches should provide support across the product lifecycle.

Reducing perceived vulnerability arising from using technology may increase the adoption of smart home technology but may also contribute to more insecure behaviour as a result if not managed appropriately. An approach that focuses on helping consumers to feel able to effectively manage any potential vulnerabilities that emerge rather than simply influencing perceptions of threat is likely to be preferable, and will also assist in building consumer resilience to emerging security risks as technology develops (e.g. Brass & Sowell, 2020; van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019). Such an approach will likely require flexible and adaptive engagement with the community, or other trusted and accessible, support mechanisms. Such approaches should provide support across the product lifecycle.

Although risk information may increase secure behaviour it may also reduce intentions to use such devices. Therefore, exposure to media information regarding the risks of smart home technologies should be accompanied by protective information that educates consumers on how they can easily manage these risks to increase secure behaviour without reducing usage or adoption of devices. Such information would likely benefit from the responsive, coordinated, and adaptive approaches typically seen in effective online crisis communications (e.g. Roshan, Warren & Carr, 2016).

Privacy and security work in slightly different ways and this requires more investigation. In the current work, although explicitly priming people to focus on security improved security behaviours, it appeared to have an adverse impact on privacy behaviours. On the other hand, implicitly priming people to focus on privacy behaviours improved both privacy and security behaviours. As such, interventions in the smart home context should be carefully considered regarding the particular behaviour that they are aiming to encourage and the wider impacts that they may have on related behaviours.

READ MORE

Agarwal, R., & Prasad, J. (2007). Are individual differences germane to the acceptance of new information technologies? *Decision Sciences, 30,* 361–391

Ali, B., & Awad, A. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors (Switzerland), 18(3)

Ballantyne, D. (2003). A relationship-mediated theory of internal marketing. *European Journal of Marketing, 37*, 1242–1260

Bashir, A., & Mir, A. (2018). Internet of things security issues, threats, attacks and counter measures. International Journal of Computing and Digital Systems, 7(2), 111–120

BBC News (2018). *Panorama's Hacked: Smart Home Secrets*. Accessed from *https://www.bbc.co.uk/news/av/uk-44117337/security-footage-viewed-by-thousands*

Beautement, A., Sasse, A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. *Proceedings of the 2008 New Security Paradigms Workshop*, California, USA, 22-25 Sep, 47–48

Blythe, J.M., & Johnson, S.D. (2019). A systematic review of crime facilitated by consumer Internet of Things. *Security Journal,* doi:10.1057/s41284-019-00211-8

Brass, I., & Sowell, J.H. (2020). Adaptive governance for the Internet of Things: Coping with emerging security risks. *Regulation & Governance,* doi:10.1111/rego.12343

Coughlin, J.F., D'Ambrosio, L.A., Reimer, B., & Pratt, M.R. (2007). Adult perceptions of smart home technologies: Implications for research, policy & market innovations in healthcare. *Proceedings of the 29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society,* Lyon, France, 22–26 August.

Das, S., Kim, A., Jelen, B., Streiff, J., Camp, L.J., & Huber, L. (2020). Why don't older adults adopt two-factor authentication. *Proceedings of the 2020 SIGCHI Workshop on Designing Interactions for the Ageing Populations - Addressing Global Challenges*. Available at: *https://ssrn.com/abstract=3577820*

de Boer, P., van Deursen, A., & van Rompay, T. (2019). Accepting the Internet-of-Things in our homes: The role of user skills. *Telematics and Informatics, 36*, 147–156

Dewnarain, S., Ramkissoon, H., & Mavondo, F. (2019). Social customer relationship management: An integrated conceptual framework. *Journal of Hospitality Marketing & Management, 28,* 172–188.

Featherman, M.S., & Pavlou, P.A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59,* 451-474

Hadlington, L., & Chivers, S. (2018). Segmentation analysis of susceptibility to cybercrime. Exploring individual differences in information security awareness and personality factors. *Policing: A Journal of Policy and Practice, 14*, 6, 479–492

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R.J., Filippoupolitis, A., & Roesch, E. (2018). A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security, 78,* 398–428

Hubert, M., Blut, M., Brock, C., Zhang, R. W., Koch, V., & Riedl, R. (2019). The influence of acceptance and adoption drivers on smart home usage. *European Journal of Marketing, 53,* 6, 1073–1098

Jugend, D., Ribeiro de Araujo, T., Pimenta, M.L., Gobbo, J.A., & Hilletofth, P. (2017). The role of cross-functional integration in new product development: Differences between incremental and radical innovation projects. *Innovation: Organization & Management, 20,* 42–60

Kadic-Maglajlic, S., Boso, N., & Micevski, M. (2018). How internal marketing drives customer satisfaction in matured and maturing European markets? *Journal of Business Research, 86*, 291–299.

Key, T.M., & Czaplewski, A.J. (2017). Upstream social marketing strategy: An integrated marketing communications approach. *Business Horizons, 60,* 325–333

Kim, K.J., & Shin, D-H. (2015). An acceptance model for smart watches: Implications for the adoption of future wearable technology. *Internet Research, 25,* 527–541

Lin, C-H., Shih, H-Y., & Sher, P.J. (2007). Integrating technology readiness into technology acceptance: The TRAM model. *Psychology & Marketing, 24,* 641–657

Mani, Z. & Chouk, I. (2018). Consumer resistance to innovation in services: Challenges and barriers in the Internet of Things era. *Journal of Product Innovation Management, 35*, 780–807

Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. *Technological Forecasting and Social Change, 138*, 139–154

McGuire, M. & Dowling, S, (2013). *Cyber crime: A review of the evidence*. Home Office research report 75. Available: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf*

NCSC (2019). *Smart devices in the home*. Accessed from *https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home*.

Nicholson, J., Coventry, L., & Briggs, P. (2019). "If it's important, it will be a headline": Cybersecurity information seeking in older adults. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 349,* 1–11

Nikou, S. (2019). Factors driving the adoption of smart home technology: An empirical assessment. *Telematics and Informatics, 45,* DOI: 10.1016/j.tele.2019.101283

Patton, J. H., Stanford, M. S., & Barratt, E. S. (1995). Factor structure of the Barratt impulsiveness scale. *Journal of Clinical Psychology*, *51*, 768–774

Park, C., Kim, Y., & Jeong, M. (2018). Influencing factors on risk perception of IoT-based home energy management services. *Telematics and Informatics, 35,* 2355–2365

Ratchford, M., & Barnhart, M. (2012). Development and validation of the technology adoption propensity (TAP) index. *Journal of Business Research*, *65*, 1209–1215

Roshan, M., Warren, M., & Carr, R. (2016). Understanding the use of social media by organisations for crisis communication. *Computers in Human Behavior, 63,* 350–361

Shin, J., Park, Y., & Lee, D. (2018). Who will be smart home users? An analysis of adoption and diffusion of smart homes. *Technological Forecasting & Social Change, 134,* 246–253

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34,* 3, 487–502

Sovacool, B.K., & Furszyfer Del Rio, D.D. (2020). Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies. *Renewable and Sustainable Energy Reviews, 120,* 109663.

Statista (2018a). *Size of the IoT market worldwide from 2016 to 2020*. Cited from *https://www.statista.com/statistics/764051/iot-market-size-worldwide/*

Statista (2018b). *Control and connectivity smart home household penetration rate in the United Kingdom (UK) from 2016 to 2022*. Cited from *https://www.statista.com/statistics/483847/home-automation-smart-home-household-penetration-digital-market-outlook-uk/*

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 123,* 29–39

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior, 78,* 283–297

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75,* 547–559

Wahlberg, A.A.F., & Sjoberg, L. (2000). Risk perception and the media. *Journal of Risk Research, 3,* 31–50

Weber, E.U., Blais, A.-R., & Betz, N. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making, 15,* 263–290

Williams, E.J., Hinds, J., & Joinson, A.N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies, 120,* 1–13

Williams, E.J., & Joinson, A.N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity, 6*, tyaa001.

Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy, 103,* 72–83

Wünderlich, N., Wangenheim, F., & Bitner, M. (2013). High tech and high touch: A framework for understanding user attitudes and behaviors related to smart interactive services. *Journal of Service Research, 16*, 3–20

Yang, H., Lee, H., & Zo, J. (2017). User acceptance of smart home services: An extension of the Theory of Planned Behavior. *Industrial Management & Data Systems, 117*, 68–89

For more information on CREST
and other CREST resources, visit
www.crestresearch.ac.uk

CENTRE FOR RESEARCH AND
EVIDENCE ON SECURITY THREATS

21-012-02