# Maintaining cyberhygiene in the Internet of Things (IoT): An expert consensus study of requisite user behaviours


## Abstract

The Internet of Things (IoT) connects computing devices embedded in everyday objects via the internet, enabling them to send and receive data. Little is known about behaviours required to protect IoT users. The study sought to develop expert consensus on the key protective behaviours, risk behaviours, and threats for IoT cybersecurity. An online, three-round Delphi consensus study was conducted with IoT experts. In Round One, experts' responses to open-ended questions were analysed using inductive and content analyses to categorise them into behavioural categories. In Round Two, experts rated the importance of protective behaviours, and the likelihood that risk behaviours and threats would lead to IoT breaches. In Round Three experts re-evaluated their responses based on their own and the group's responses. Experts agreed that 28 protective behaviours, one risk behaviour, and six threats were critical for IoT cyberhygiene. Five of the top 10 protective behaviours for conventional computing were also deemed important for IoT, i.e. '*Limit sharing of your personal information with devices'*, *'Keep your IoT devices updated'*; *'Read articles about IoT security, safety and privacy risks', 'Use a strong firewall', and 'Use strong passwords on devices, networks and services*'. The study provided information on the key behaviours and threats for IoT settings, and the extent to which recommendations for conventional computing settings may also be suitable for IoT settings. These findings can inform the development of tailored behaviour change interventions to improve cybersecurity.



**Keywords:** Cyberhygiene; Cybersecurity; Internet of things; Protective behaviour; Risk behaviour; Threat.


## Declarations of interest

The authors do not have any conflicts of interest to report.

Abbreviations
IoT: Internet of Things; IQR: Interquartile Range


https://doi.org/10.32388/KIR04H

## Introduction

The Internet of Things (IoT) connects the internet and everyday electronic objects, including smart technologies embedded in wearables (such as smart watches) and household appliances (such as home hubs) (Government Office for Science, 2014; Lee & Lee, 2015). While increased connectedness may streamline daily activities, it also increases the risk of security and privacy concerns from innovative and sophisticated threats. Attackers may use a variety of resources and techniques in order to access and exploit deficient protective mechanisms. Such deficiencies may include devices lacking digitally-signed software updates, unencrypted storage of passwords on users' Wi-Fi networks and default administrative passwords on devices (Dragoni et al., 2015).

Cybercrimes are increasingly becoming one of the most common offenses worldwide. For example, in 2016 an estimated two million instances of cybercrime were reported in the UK alone (Office for National Statistics, 2016). In 2017 an estimated 16.7 million US citizens had a collective $16.8 billion stolen from them by cybercrime, with this being an eight percent increase in the number of victims from 2016 (Pascual et al., 2018). As a consequence, increasing the innovation and adoption of secure and resilient IoT protections has become a key global priority for Governments (Joo et al., 2018).

Cybersecurity focuses on interactions between organisations, devices and citizens (Von Solms & Van Niekerk, 2013). Vishmanath *et al.* (2020) defined *'Cyberhygiene' as "*the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet enabled devices from being compromised in a cyber-attack*."* Maintaining cyberhygiene requires a complex combination of technical, procedural and behavioural approaches to combat or mitigate threats (Uckelmann et al., 2011). High profile instances of security *'Threats'* (such as ransomware and phishing emails) have been met with surveillance efforts to protect users (Craggs & Rashid, 2017), and increasing pressure has been placed upon IoT manufacturers to protect devices and ultimately users (Federal Trade Commission, 2015). However, protection and privacy mechanisms against online threats lag behind innovation and growth in IoT technology (Lee & Lee, 2015) as well as the ability to protect against increasingly sophisticated and rapidly evolving threats (Craggs & Rashid, 2017). Currently there is no consensus among experts on what the key threats facing IoT users are; this further leaves the security and privacy of users' information at risk of access and exploitation (Bullguard, 2016).

Understanding and changing IoT users' behaviours is key to maintaining and enhancing cyberhygiene in the face of technical and procedural difficulties. These may include cyber-behaviours like setting up a firewall, and non-cyber (physical) behaviours like purchasing a specific device. A behavioural perspective is required to appraise what protective steps can reasonably be expected from IoT users and which problems are needed to be solved through a security-by-design approach. Understanding behaviour is required to enhance device design relating to user capabilities, goals and values (Sasse, 2015), reduce user time and effort burden (Herley, 2014), and ensuring security application and advice is actionable in the light of other important and/or competing behaviours (Coventry et al., 2014; Craggs & Rashid, 2017). Furthermore, understanding such behaviours can help shape advice to users to help avoid common pitfalls of advice appearing contradictory, difficult to follow and/or not appropriate (Coventry *et al.,* 2014), ensure that advice fits as much as possible with existing behaviours or behavioural factors (Michie et al., 2011; Michie et al., 2014), and guide IoT device design Coventry *et al.,* 2014; Craggs & Rashid, 2017).

Broadly, there are two types of user behaviour enabling IoT cyberhygiene. *'Protective'* behaviours are actions that protect users' security, privacy and safety. These are important at all stages in the IoT device '*Lifecycle*' (i.e. periods between device development and disposal), and may include researching device security before purchase, password maintenance following purchase, or safe disposal once no longer in use. *'Risk'* behaviours are actions that increase the likelihood of cybersecurity difficulties or breaches. These may be not engaging in protective behaviours such as not changing passwords, or direct actions such as accessing illegal websites.

Measures aimed at increasing protective behaviours and reducing risk behaviours include education and training users about cybersecurity (Puhakainen & Siponen, 2010), enhancing usability of, or nudging users, towards security features and targeting design failures (Adams & Sasse, 1999; Camp, 2011; Coventry et al., 2016; Furnell, 2007; Sasse, 2015; Turland et al., 2015). However, behavioural changes relating to security measures have proved challenging to implement due to issues such as devices not providing a standard method for applying security updates, or users circumventing security methods to focus on their primary task (e.g. social networking) (Beautement et al., 2009).

In order to understand what constitutes best practice, and for researchers to design and implement behaviour change interventions aimed at enhancing cyberhygiene, it is necessary

to understand both the key behaviours and the nature of the threats relating to cybersecurity (Michie, *et al.*, 2011, 2014). For example, IoT device designers who have the goal of improving the security of users' devices have to address many user behaviours, such as setting secure passwords, manually running antivirus checks and using only secure Wi-Fi connections. Each of these will be associated with particular situations and require particular capabilities, as well as being more or less motivating for users. By increasing the understanding of user behaviours, and their contexts and influences, IoT designers will be better equipped to design devices and procedures that promote user engagement in protective behaviours and reduce risk behaviours.

Ten 'behavioural best practices' for general (rather than IoT-specific) cyberhygiene have been outlined by the UK Government (Coventry *et al.*, 2014). These were generated from an analysis of cyberhygiene literature using a Rapid Evidence Assessment and checking conclusions with cybersecurity experts. The authors of the report noted that there was scope for improvement in users' cyberhygiene-related behaviours and that the behavioural research was non-systematic. In order to inform interventions to improve IoT cybersecurity, evidence is needed about IoT experts' views about key protective behaviours, risk behaviours, and threats for IoT devices.

Expert views can be efficiently gathered and consensus built using the Delphi method. This method is helpful for investigating complex issues such as IoT security where devices, users and the environment interact and where there is a dearth of high quality empirical research (Lee & Lee, 2015). The Delphi method involves recruiting experts in a specific field to respond to questions in more than one round, each building on the previous. The first round identifies issues that experts perceive to be important for a specific topic. Subsequent rounds are used to provide information about the group's views and ask participants to reconsider their views in the light of this, providing numerical ratings which are used in the consensus-building process (Iqbal & Pipon-Young, 2009). This study used the Delphi method to investigate and develop consensus amongst IoT experts on how users can maintain cyberhygiene in the IoT, particularly in terms of key protective behaviours, risk behaviours, and threats.

## Method

### Study Design & Setting

The study used a mixed-methods Delphi consensus design (Iqbal & Pipon-Young, 2009). This approach is characterised by four key features: (i) participants are selected based on expertise, (ii) a first round is used to identify a range of salient issues on the target topic, (iii) at least one questionnaire based on first round responses is used to generate consensus on the importance of key themes, and (iv) at least one evaluation round is used where both participant's own and overall participants' responses are presented and responses re-evaluated.

**Participants**

The study received ethical approval from the Psychology and Language Sciences Department at University College London, UK (9461/001). Informed consent was obtained from all participants for experimentation with human subjects. To be eligible for inclusion in the study as an 'IoT security expert', two criteria needed to be met. First, participants were required to rate their level of knowledge and expertise in 'IoT' and/or 'information security' as being equal to or greater than 4 on a scale of 0 ('*No knowledge/expertise'*) to 7 ('*Profound knowledge/expertise'*). Second, participants' ratings needed to be validated by an internet search by study authors' (JB; CL). No further inclusion/exclusion criteria were applied.

Fifty-three (95%) of 56 potential IoT experts who expressed an interest in participating satisfied the inclusion criteria. Out of these, thirty-four experts participated in the study (64%), of which 31 (91%) completed all three Delphi rounds. Participants were predominantly female (82% female; 15% male; 3% other), from the UK (76% UK; 24% other), and from the commercial sector (47% commercial; 29% university; 18% public; 6% voluntary). Participants had a mean of 43 years of age (range = 27-66; SD = 10) and 14 years of professional tenure (range = 1-32; SD 10.6). Participants rated themselves to be above average (≥4) for knowledge of *'Information security'* (M=5.8, SD=1.4), '*Usable security'* (M=5.2, SD=1.6), IoT (M=5.9, SD=1.3), *'Governance, risk and compliance'* (M=5.4, SD=1.7), and *'IoT security'* (M=5.1, SD=1.6), but not *'Behavioural science'* (M=3.8, SD=1.6) or *'Human-computer interaction'* (M=3.7, SD=1.7).

**Procedure**

A snowball recruitment method was used, beginning with inviting potential experts via mailing lists, websites, online forums and social media platforms (e.g. Twitter, LinkedIn) to participate in a study "*To understand user protective behaviour in the Internet of Things*". Participants were provided with study information and asked to share information about the

study on their social media platforms to widen the recruitment net. Participants were asked to complete three, consecutive Delphi rounds: (i) qualitative idea generation (Delphi Round One); (ii) quantitative consensus generation (Delphi Round Two); and (iii) quantitative consensus re-evaluation (Delphi Round Three). Questionnaires for all rounds were designed to require a maximum of 30 minutes to complete, disseminated online using Qualtics®, and were accessible for one month. Follow-up reminders were sent weekly, two days before the survey closed, and finally on the day that the survey closed.

***Qualitative Idea Generation (Delphi Round One)***

Round One was a qualitative, open-ended questionnaire (*Appendix A*) asking about potential protective behaviours, risk behaviours and threats in the IoT. A questionnaire was developed and piloted with three IoT experts who provided qualitative feedback on the wording and flow of questions, which was used to refine the questionnaire for use in Delphi Round One. The questionnaire comprised: (i) Study information explaining that the study focussed on IoT cyberhygiene behaviours and may involve current and future, and cyber and non-cyber (physical), behaviours, (ii) definitions and examples of IoT cyberhygiene target behaviours, and (iii) open-ended questions about key protective behaviours, risk behaviours, and threats. Following IoT experts responses, in order to ensure adequate coverage of potential IoT behaviours, online (Google®) searches were conducted by the researchers (JB; CL) for: (i) *"Protect yourself internet of things"*, (ii) *"Protect internet of things"*, (iii) *"Secure internet of things"*, and (iv) *"Advice internet of things"*.

Round One data was analysed using both inductive analysis (Elo & Kyngäs, 2008) and content analysis (Hsieh & Shannon, 2005). Responses were read word-for-word to derive themes and meaningful categories that were labelled to develop an initial coding scheme, which was refined as the analysis proceeded. Where participants' responses did not indicate behaviours, these responses were removed. Allocation to categories was independently coded by two researchers (JB; CL) using NVivo11™ (QSR International Pty Ltd., 2012). Inter-rater agreement was assessed by two researchers (JC; CL) using Kappa co-efficient, whereby values of 0.21-0.4 are considered 'Fair', 0.41-0.6 'Moderate', 0.61-0.8 'Substantial', and over 0.8 'Almost Perfect' (McHugh, 2012). Discussions were conducted between authors (JB; CL) until agreements were reached. Inter-rater agreement was 'Substantial' (k=0.7) (McHugh, 2012).

Responses were allocated to one of three pre-defined cyberhygiene categories: (i) *'Protective behaviours'*, (ii) *'Risk behaviours'*, or (iii) *'Threats'*. A content analysis was conducted which determined experts had provided a high number of responses about protective behaviours, but few for risk behaviours or threats. As Delphi Rounds Two and Three required a manageable amount of data for the development of quantitative questions, and to the researchers' knowledge there was no standardised criteria within the literature for how to reduce the amount of data to a manageable level, different inclusion criteria were agreed between two researchers (JB; CL). For risk behaviours and threats, due to the relatively low frequency of responses, the only criteria applied for inclusion in Delphi Round Two was a minimum threshold frequency was 12% (n = 3).

For protective behaviours the high number of responses required a three-stage item selection procedure. First, a minimum threshold frequency of 6% (n = 2) for experts' responses, and 20% (n = 3) for online sources, was applied. Secondly, a content analysis was conducted to determine potential sub-groups of protective behaviours to increase understanding and usability of data. Protective behaviours were grouped based on the most relevant IoT device '*Lifecycle*': (i) *'Pre-Purchase'*, (ii) *'Set-up & Maintenance'* or (iii) *'Disposal'*. Where a lifecycle stage had fewer than 10 behaviours, two researchers (JB; CL) either developed further items or selected those deemed most relevant from those which did not meet the Delphi Round One inclusion threshold. Two items were added to pre-purchase ("*Buy devices that allow passwords and for the default password to be changed"; "Only buy devices that can be updated if a security issue is identified*"), and three to disposal ("*Perform a factory reset on devices before disposal, where possible"; "Securely wipe devices before disposal, where possible"; "Send devices to a secure disposal facility*"). Finally, two researchers (JB; CL) assessed experts' responses and online advice for gaps in coverage and four protective behaviours were added to reflect current IoT issues *("Keep personal devices out of workplace"; "Use online IoT scanner"*) and coping strategies *("Write down password if needed"; "Use a password manager"*).

***Quantitative Consensus Generation (Delphi Round Two)***

A quantitative questionnaire was presented to experts with the aim of generating consensus on the key protective behaviours, risk behaviours and threats in the IoT. First, protective behaviours were separated into one of three IoT lifecycle stages out of: (i) *'Pre-Purchase'*, (ii) *'Set-up & Maintenance'* or (iii) *'Disposal'*. Experts were asked to rate behaviours in

terms of importance on a seven-point Likert scale, ranging from 1 (*'Not at all important')* to 7 (*'Extremely important').* Secondly, experts were asked to rate the percentage likelihood of identified risk behaviours and threats resulting in security breaches, ranging from 0% (*'Extremely unlikely')* to 100% (*'Extremely likely').* Thirdly, panel median and consensus scores were calculated for each item using Interquartile Range (IQR) scores, with smaller IQR scores indicating greater consensus (Von Der Gracht, 2012). For protective behaviours an IQR <1 was deemed to indicate *'Consensus'*, 1-2 *'Approaching consensus'*, and >2 *'No consensus'* (Raskin, 1994; Rayens & Hahn, 2000). For risk behaviours and threats an IQR <2 was deemed to indicate *'Consensus'*, 2-4 *'Approaching consensus'*, and >4 *'No consensus'* (Scheibe et al., 1975).

### *Quantitative Consensus Re-Evaluation (Delphi Round Three)*

A quantitative questionnaire was presented to experts with the aim of re-evaluating scores for protective behaviours, risk behaviours and threats for which consensus was not previously reached. All items for which consensus had been reached in Round Two were provided for reference only. Items for which consensus had not been reached were presented alongside information about: (i) the participant's individual scores, (ii) the overall expert sample's median scores and frequency graphs, and (iii) the overall expert sample's IQR consensus scores. Participants were asked to re-evaluate their scores in light of this additional new information, and had the opportunity to provide optional qualitative explanations for changes in their scores between Rounds Two and Three.

## Results

### Qualitative Idea Generation (Delphi Round One)

Of the 34 participants, 32 (94%) provided responses for protective behaviours, 25 (74%) for risk behaviours, and 25 (74%) for threats. Sixty-two potential protective behaviours were discussed, which were supplemented by a further 92 from 15 online sources. Experts also discussed 40 potential risk behaviours and 47 threats. While online sources were also examined for potential risk behaviours and threats no additional items were identified to supplement those discussed by IoT experts.

### Quantitative Consensus Generation (Delphi Round Two)

In Delphi Round Two, experts were presented with the 43 protective behaviours, nine risk behaviours and 12 threats discussed during Delphi Round One that satisfied the selection

criteria for inclusion in the quantitative questionnaire (*Appendix B*). Experts were asked to rate the importance of each item. Of 43 potential risk behaviours experts reached consensus for 23 (53%), approached consensus for 15 (35%), and did not reach consensus for five (12%). Of nine potential risk behaviours experts reached consensus for zero (0%), approached consensus for two (22%), and did not reach consensus for seven (78%). Of 12 potential threats experts reached consensus for zero (0%), approached consensus for eight (67%), and did not reach consensus for four (33%).

## Quantitative Consensus Re-Evaluation (Delphi Round Three)

In Delphi Round Three experts were presented with the 20 protective behaviours, 9 risk behaviours and 12 threats for which consensus was not reached in Round Two and asked to re-evaluate their scores in light of new, additional information regarding their own and the overall expert sample's scores from Delphi Round Two. Consensus scores and comparisons between the expert sample's ratings for Delphi Rounds Two and Three are presented in *Table 1* for protective behaviours, and *Table 2* for risk behaviours and threats.

**Table 1:** *Comparisons between experts' mean and Interquartile Range consensus scores for Delphi Rounds Two and Three – Protective behaviours (with those for which consensus was reached by the end of Round Three in bold)*

| **IoT Protective Behaviour** | | | **Round Two (n = 33)** | | **Round Three (n = 31)** | |
|---|---|---|---|---|---|---|
| **Lifecycle** | **Domain** | **Sub-Domain** | **Mean[a] (SD)** | **IQR[b]** | **Mean[a] (SD)** | **IQR[b]** |
| **Pre-Purchase** | | Buy and use product and services from reputable companies | 5.67 (1.34) | 2 | 6.03 (1.02) | 2 |
| | | **Buy devices that allow passwords and for the default password to be changed** | **6.3 (.98)** | **1** | | |
| | | **Buy devices that can work without the cloud** | **5.36 (1.29)** | **1** | | |
| | | **Buy devices with security-focused platforms (e.g. Apple HomeKit, Samsung SmartThings)** | **5.85 (1.06)** | **2** | **5.71 (1.27)** | **1** |
| | | **Decide whether considered IoT device is ideal for its intended purpose** | **5.94 (1.17)** | **2** | **6.16 (.90)** | **1** |
| | | Minimise the number of different IoT device providers that you buy from | 4.45 (1.86) | 3 | 4.48 (1.75) | 3 |
| | | **Only buy devices that can be updated if a security issue is identified** | **6.06 (1.14)** | **1** | | |
| | | **Research the security of the IoT device before purchasing** | **6.21 (1.05)** | **1** | | |
| **Set-up & Maintenance** | **Credential Management** | **Change the default passwords on devices, networks and services** | **6.91 (.29)** | **0** | | |
| | | **Don't re-use your passwords on devices, networks and services** | **6.33 (.82)** | **1** | | |
| | | **Don't share your passwords** | **6.52 (1.03)** | **1** | | |
| | | Regularly change passwords on devices, networks and services | 5.64 (1.8) | 2 | 5.42 (1.84) | 3 |
| | | Set-up account lock-out following failed password attempts, where possible | 6.0 (1.15) | 2 | 6.1 (1.11) | 2 |
| | | Use a password manager application | 5.45 (1.62) | 3 | 5.81 (1.25) | 2 |
| | | **Use multi-faceted/two-step authentication, where possible** | 6.33 (.78) | 1 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | **Use strong passwords on devices, networks and services** | **6.7 (.59)** | **0** | | |
| | | Write down passwords if needed | 3.09 (1.96) | 4 | 3.23 (1.78) | 2 |
| | **Network Management** | Disable "Universal Plug and Play (UPnP)" on your router | 5.48 (1.25) | 2 | 5.68 (1.19) | 2 |
| | | **Ensure that your Wi-Fi is secure to at least WPA2 level** | **6.58 (.56)** | **1** | | |
| | | **Isolate IoT devices onto their own network** | **5.27 (1.31)** | **1** | | |
| | | Limit the number of connected devices and disconnect devices that no longer need an active connection | 5.58 (1.54) | 2 | 5.77 (1.45) | 2 |
| | | **Monitor network traffic on your router** | **5.58 (1.3)** | **2** | **5.39 (1.17)** | **1** |
| | **Device Settings** | **Modify the privacy and security settings of the device in line with your needs** | **6.48 (.62)** | **1** | | |
| | | **Understand and learn the system configuration and settings** | **5.73 (1.23)** | **2** | **5.77 (1.12)** | **0** |
| | **Privacy protections** | **Limit or disable the amount of information that the devices shares across networks and services to the minimum necessary** | **6.27 (.91)** | **1** | | |
| | | **Limit sharing of your personal information with devices** | **6.3 (.81)** | **1** | | |
| | | Read and understand the terms and conditions | 5.64 (1.45) | 2 | 5.39 (1.65) | 3 |
| | **Updating** | Install updates as soon as they become available | 5.85 (1.5) | 2 | 6.03 (1.38) | 2 |
| | | **Keep your IoT devices updated** | **6.33 (1.14)** | **1** | | |
| | | Select "automatically update" when possible | 5.39 (1.92) | 2 | 6.06 (1.21) | 2 |
| | | **Set a schedule to check for updates if "automatic update" is not available** | **5.73 (1.61)** | **1** | | |
| | **Other** | **Enable encryption of communications and data, where possible** | **6.42 (.83)** | **1** | | |
| | | Keep your personal devices off the workplace network | 4.94 (1.69) | 2 | 4.9 (1.62) | 2 |
| | | Only use authorised software/services with your IoT devices | 5.73 (1.42) | 2 | 5.61 (1.54) | 2 |
| | | **Read and familiarise yourself with the manufacturer's instructions during installation** | **5.7 (1.19)** | **2** | **5.65 (1.17)** | **1** |
| | | **Read articles about IoT security, safety and privacy issues** | **5.33 (1.41)** | **1** | | |
| | | **Use a strong firewall** | **6.18 (.98)** | **1** | | |
| | | Use online IoT scanners to check for vulnerabilities (such as Bullguard) | 5.24 (1.56) | 3 | 4.97 (1.49) | 2 |
| **Disposal** | | Discard devices that have security weaknesses that can't be fixed | 6.03 (1.19) | 2 | 6.06 (1.34) | 2 |
| | | **Perform a factory reset on devices before disposal, where possible** | **6.42 (.75)** | **1** | | |
| | | **Remove unsafe devices from the network** | **6.61 (.5)** | **1** | | |
| | | **Securely wipe devices before disposal, where possible** | **6.36 (.78)** | **1** | **6.81 (.40)** | **0** |
| | | **Send devices to a secure disposal facility** | **5.58 (1.23)** | **2** | **5.58 (1.06)** | **1** |

[a]**Scale:** 1 '*Not at all important'* to 7 '*Extremely important'*
[b]**Consensus:** IQR<1 '*Consensus'*; 1<IQR<2 '*Approaching consensus'*; IQR<2 '*No consensus'*

**Table 2:** *Comparisons between experts' mean and IQR consensus scores for Delphi Rounds Two and Three – Risk behaviours and threats (with those for which consensus was reached by the end of Round Three in bold)*

| **IoT Behaviour** | | **Round Two (n=33)** | | **Round Three (n=31)** | |
|---|---|---|---|---|---|
| **Behaviour** | **Sub-Domain** | **Mean %[a] (SD)** | **IQR[b]** | **Mean %[a] (SD)** | **IQR[b]** |
| **Risk Behaviour** | Choosing weak passwords | 60% (31) | 5 | 66% (21) | 3 |
| | Disabling security features | 69% (26) | 5 | 75% (20) | 3 |
| | **Not changing the default password** | **71% (28)** | **5** | **85% (16)** | **1** |
| | Not changing the default settings on devices | 53% (31) | 5 | 58% (25) | 4 |
| | Not installing software updates | 64% (27) | 5 | 69% (23) | 4 |
| | Password re-use | 50% (31) | 5 | 56% (26) | 4 |
| | Placing convenience before security | 65% (26) | 4 | 71% (19) | 3 |
| | Sharing of too much personal data | 58% (31) | 6 | 64% (27) | 5 |
| | Visiting risky websites (such as torrent websites) | 66% (26) | 3 | 72% (22) | 4 |

| | | | | | |
|---|---|---|---|---|---|
| **Threats** | Botnets | 50% (27) | 5 | 55% (20) | 3 |
| | **Compromised control devices (e.g. driving)** | **23% (22)** | **3** | **18% (15)** | **2** |
| | Compromised safety critical alerting devices (e.g. smoke alarms) | 25% (22) | 3 | 22% (20) | 3 |
| | **Counterfeiting (e.g. fake replicas of IoT products)** | **36% (24)** | **3** | **33% (20)** | **2** |
| | Data mining and harvesting | 59% (27) | 4 | 64% (22) | 3 |
| | Denial of service | 36% (26) | 4 | 35% (24) | 3 |
| | Eavesdropping | 41% (26) | 5 | 43% (21) | 3 |
| | **Malware** | **69% (21)** | **3** | **74% (19)** | **2** |
| | **Man in the middle attacks** | **37% (24)** | **4** | **36% (2)** | **2** |
| | **Physical tampering of devices** | **21% (20)** | **5** | **17% (16)** | **2** |
| | **Social engineering (e.g. phishing)** | **74% (24)** | **5** | **81% (19)** | **2** |
| | Tracking users | 71% (28) | 3 | 76% (23) | 3 |

[a]**Scale:** 0% '*Highly unlikely'* to 100% '*Highly likely'*

[b]**Consensus:** IQR<2 '*Consensus*'; 2<IQR<4 '*Approaching consensus'*; IQR<4 '*No consensus'*

In Round Three IoT experts reached consensus for 28 (65%), approached consensus for 12 (28%), and did not reach consensus for three (7%) of 43 protective behaviours. The behaviours which reached greatest consensus for each IoT device lifecycle stage were '*Pre-purchase: "Buy devices that allow passwords and for the default password to be changed"*', '*Set-up & Maintenance: "Changing the default passwords on devices, networks and services"*', and '*Disposal: "Remove unsafe devices from the network"'*. IoT experts reached consensus for only one of nine risk behaviours (11%): *"Not changing the default password"*. Experts approached consensus for seven risk behaviours (78%) and did not reach consensus for the remaining one (11%). IoT experts reached consensus for six threats (50.00%) and approached consensus for the remaining six (50%). IoT threats relating to *'Social engineering'* and *'Malware'* were considered the most likely to lead to breaches.

Experts either approached or did not reach consensus for 35% of protective behaviours, 89% of risk behaviours, and 50% of threats. In certain instances not reaching consensus reflected experts having different views on whether protective behaviours, risk behaviours or threats had positive, negative, or no discernible impact upon cyberhygiene. An example of this was for the protective behaviour "*Minimise the number of different IoT device providers that you buy from*". Certain experts believed that conducting this behaviour would be protective as *"Choosing more providers can expose you to more varied risks…"*. However, others viewed that this would not be protective as *"Reducing the number of providers only stimulates retaining the current soloed and fragmented IoT landscape"*. There were also instances where experts considered specific behaviours to potentially have both positive and negative effects depending upon the scenario. An example of this was for the protective behaviour *"Regularly change passwords on devices, networks and services"*. Certain experts highlighted that this protective behaviour could also put users at risk as *"…forcing password*

*changes on a set schedule is a bad thing, as it encourages users to pick easily guessed passwords…".*

## Discussion

Experts reached consensus about the importance of 28 (of 43) protective behaviours, one (of nine) risk behaviour(s), and six (of 12) threats for IoT user cybersecurity. Of the 10 'behavioural best practices' for maintaining cybersecurity in conventional computing settings (Coventry et al., 2014) five were found in this study to be considered important in IoT settings (i.e.: "*Limit sharing of your personal information with devices", "Keep your IoT devices updated", "Read articles about IoT security, safety and privacy risks", "Use a strong firewall",* and *"Use strong passwords on devices, networks and services*". This suggests that it may be desirable to develop some generic cyberhygiene practices across settings rather than having all tailored specifically to IoT settings. This would have the advantage of users not being required to understand and apply different behaviours in different situations or settings. Future research is required to assess the pros and cons of applying setting-specific versus generic cyberhygiene recommendations to understand the degree to which tailoring is required.

Three of the five other key conventional computing behaviours (Coventry et al., 2014) were found amongst the 43 potential protective behaviours identified by IoT experts in the current study (i.e. *"Log out of sites after you have finished and shut down your computer", "Use only trusted and secure connections, computers and devices (including Wi-Fi)",* and *"Use only trusted and secure sites and services").* However, experts did not reach consensus about their importance. This discrepancy may reflect differences between the settings as, while conventional computing (such as desktop computers) may require more systematic use and application, IoT devices (such as smart hubs) are designed to interact with the physical environment. This may influence the perceived relevance or possibility of conducting these more deliberate, planned behaviours for IoT technologies which may be designed (at least partly) for the purpose of negating the need for them (Government Office for Science, 2014). For example, smart hubs are designed to connect home devices at all times, and as such logging out once tasks are finished would reduce its functionality. This appeared to be supported by qualitative feedback from experts which highlighted uncertainty or discrepancies in beliefs about whether behaviours could and should be applied in IoT settings as well as whether certain behaviours themselves would be protective and/or risky.

Two of the 10 key conventional computing cyberhygiene behavioural recommendations (Coventry et al., 2014) were not identified by experts in the current study. This may reflect differences in what is perceived to be actionable or necessary in the IoT. *"Be aware of your physical surroundings when online"* in conventional computing reflected the need for users to be vigilant in public spaces and ensure computers and mobiles are locked when unattended. As using IoT devices fundamentally involves interacting with the environment and typically in order for devices to be used effectively they are required to be online most (if not all) of the time, this has low perceived relevance for IoT settings. *"Report cybercrimes and criminals to the authority"* in conventional computing reflected limited reporting of breaches and confidence in authorities to deal with them. As this behaviour is neither protective nor a risk, and instead a behavioural bi-product of being subjected to a threat, this may not have been deemed relevant by experts. These examples demonstrate the importance of developing an understanding of both the behavioural similarities and differences between IoT and conventional computing settings, and the behavioural requirements of responding should threats arise.

Contrary to protective behaviours where consensus was reached for 28 behaviours, experts agreed on only one risk behaviour. The lack of consensus may reflect a scarcity of currently available evidence, and a need for information and research relating to the role of risk behaviours contribution to cybersecurity breaches. Risk behaviours studied in previous research have included oversharing of personal information in social networks (Hadnagy, 2010), downloading illegal files (Dilmperi et al., 2011) and poor password hygiene (Whitty et al., 2015). These behaviours and an additional four identified within the study may reflect a lack of awareness or an intention to conduct risk behaviours despite awareness of the consequences. *"Not changing the default password"* was the only risk behaviour for which experts reached consensus, and is an example of the opposite of a protective behaviour. Not changing passwords was a critical component of a major and widely publicised IoT breach prior to the study commencing (Poornachandran et al., 2016), which may explain consensus on this item due to the 'availability' heuristic, where immediate information is prioritised when evaluating risks (Tversky & Kahneman, 1973).

Experts identified 12 potential IoT threats and reached consensus about six of them. As was the case for risk behaviours, experts focused on those perceived to be problematic (i.e. "Counterfeiting", "Malware", and "Social engineering") rather than newer, more advanced threats which are not (e.g. "Botnets", "Eavesdropping", "Tracking users"). This highlights the

need for research to be responsive to the rapidly developing IoT technology landscape, in order to provide guidance on new threats as they emerge.

Future research is required to develop interventions to change key protective behaviours, risk behaviours and threats. Achieving behaviour change is challenging as individual behaviours are not conducted in isolation; instead they form part of a 'system' of behaviours that influence desired outcomes (Michie, et al., 2011, 2014). By engaging in one behaviour repeatedly this may provide a platform for engaging in other behaviours. However, in instances where security advice is difficult to implement (Sasse, 2015), behaviours interfere with users' primary goals (Kirlappos et al., 2015) and/or require significant time or effort (Beautement et al., 2009) IoT device users are less likely to conduct best practice cyberhygiene behaviours. Future collaborative research with IoT users and designers is required to determine the perceived ease, likelihood and impact of specific behavioural changes considered important for maintaining cybersecurity by IoT experts. The findings of such research could be used to inform interventions that are likely to be effective.

**Study Strengths & Limitations**

The study used the validated and commonly used Delphi method (Iqbal & Pipon-Young, 2009) to identify and reach consensus on behaviours in a research area where there is a current lack of evidence and consensus. The study was designed to allow comparisons between IoT and conventional computing settings (Coventry et al., 2014). The use of a well-tested online platform Qualtics® enabled high recruitment and response rates: 64% of experts who expressed an interest in participating and satisfied the inclusion criteria took part, and 94% of experts who started the study completed it. A further strength was 'Substantial' inter-rater reliability in coding data. Despite these strengths the study was limited by the number of behaviours and threats identified by experts. This meant that additional protective behaviours were introduced from a literature review and fewer risk behaviours and threats being identified than protective behaviours.

**Conclusion**

IoT cyberhygiene currently focuses on security by design. However, as IoT devices become embedded in daily life, increased emphasis is placed upon the behavioural factors of product development, design and usage. Despite this, little is known about the behaviours that users need to maintain, or avoid, in order to mitigate cybersecurity threats. IoT experts agreed that 28 protective behaviours, one risk behaviour, and six threats are critical IoT cybersecurity. Of

the 10 key protective behaviours for conventional computing identified by previous research, five were also independently identified as important for IoT settings, but only *"Use strong passwords"* featured in the top 10 for both settings. *"Not changing the default password"* was the only risk behaviour for which experts reached consensus, and threats also present in conventional computing were perceived to be more important than newer, potentially more sophisticated IoT threats. The current study provided information about the key behaviours for IoT settings, and the extent to which recommendations may or may not be suitable for both conventional computing and IoT settings. Future research is required to determine the ease, likelihood and potential impact of targeting specific behaviours, with a view to informing interventions that promote appropriate behaviours whilst minimising user burden.

Declarations of interest

None.

**Submission declaration and verification**

The authors declare that the work has not previously been published, it is not under consideration for publication elsewhere, and its publication has been approved by all authors and authorities where the work was carried out. If accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copy-right holder.

**Funding**

This work was supported by the UK Engineering and Physical Sciences Research Council [Grant: EP/N02334X/1].

**Availability of data and materials**

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

## References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM. 42(12),* 41-46.

Beautement, A., Sasse, M. A. & Wonham, M. (2009). The compliance budget: managing security behaviour in organisations. Proceedings of the 2008 New Security Paradigms Workshop, ACM, pp. 47-58.

Bullguard. (2016). Despite Fast Adoption of Internet of Things, A Shocking 72 Per Cent Of Consumers Don't Know How To Secure Their Connected Devices. Retrieved June 1, 2019, from http://www.bullguard.com/press/latest-press-releases/2016/03-17.aspx.

Camp, L. J. (2011). Reconceptualizing the role of security user. *Daedalus, 140(4),* 93-107.

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices improve the public's use of cyber. Retrieved June 1, 2019, from http://nrl.northumbria.ac.uk/23903/.

Coventry, L. M., Jeske, D., Blythe, J. M., Turland, J., & Briggs, P. (2016). Personality and social framing in privacy decision-making: A study on cookie acceptance. *Frontiers in psychology, 7,* 1341.

Craggs, B., & Rashid, A. (2017). Smart cyber-physical systems: beyond usable security to security ergonomics by design. 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), IEEE, pp. 22-25.

Dilmperi, A., King, T., & Dennis, C. (2011). Pirates of the web: The curse of illegal downloading. *Journal of Retailing and Consumer Services, 18(2),* 132-140.

Dragoni, N., Giaretta, A., & Mazzara, M. (2016). The internet of hackable things. International Conference in Software Engineering for Defence Applications, SEDA, pp. 129-140.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of advanced nursing, 62(1), 107*-115.

Federal Trade Commission. (2015). IoT Privacy & Security in a Connected World. Retrieved June 1, 2019, from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-

privacy/150127iotrpt.pdf.

Furnell, S. (2007). Making security usable: Are things improving?. *Computers & Security, 26(6).* 434-443.

Government Office for Science. (2014). The Internet of Things: making the most of the Second Digital Revolution. Retrieved June 1, 2019, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

Hadnagy, C. (2010). Social engineering: The art of human hacking. Wiley Publishing Inc., Indiana.

Herley, C. (2014). More Is Not the Answer. *IEEE Security & Privacy, 12(1),* 14–19.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research, 15(9),* 1277-1288.

Iqbal, S., & Pipon-Young, L. (2009). The Delphi Method. *The Psychologist, 22(7),* 598–601.

Joo, M. H., Kwon, H. Y., & Lim, J. I. (2018). Cyber Security Governance Analysis in Major Countries and Policy Implications. *Journal of the Korea Institute of Information Security and Cryptology, 28(5),* 1259-1277.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). Shadow security as a tool for the learning organization. *ACM SIGCAS Computers and Society, 45(1),* 29-37.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58(4),* 431-440.

McHugh, M. L. (2012). Interrater reliability: the kappa statistic. *Biochemia medica: Biochemia medica, 22(3),* 276-282.

Michie, S., Atkins, L., & West, R. (2014). The behavior change wheel – a guide to designing interventions. Silverback Publishing, London (UK).

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science, 6(1),* 42.

Office for National Statistics. (2016). Crime in England and Wales: year ending Sept 2016. Retrieved June 1, 2019, from

https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016.

Pascual, A., Marchini, K., & Miller, S. (2018). Identity fraud: Fraud enters a new era of complexity. Retrieved June 1, 2019, from https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

Poornachandran, P., Nithun, M., Pal, S., Ashok, A., & Ajayan, A. (2016). Password reuse behavior: how massive online data breaches impacts personal data in web. In: Saini, H., Sayal, R., Rawat, S. (Eds.), Innovations in Computer Science and Engineering. Springer, Singapore, pp. 199-210.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, *34(4)*, 757-778.

QSR International Pty Ltd. (2012). NVivo Qualitative Data Analysis Software (Version 10)[Software].

Raskin, M. S. (1994). The Delphi study in field instruction revisited: Expert consensus on issues and research priorities. *Journal of Social Work Education*, *30(1)*, 75-89.

Rayens, M. K., & Hahn, E. J. (2000). Building consensus using the policy Delphi method. *Policy, politics, & nursing practice*, *1(4)*, 308-315.

Linstone, H. A., Turoff, M., & Helmer, O. (1975). The Delphi Method: Techniques and Applications. Retrieved June 1, 2019, from https://web.njit.edu/~turoff/pubs/delphibook/delphibook.pdf.

Sasse, A. (2015). Scaring and bullying people into security won't work. *IEEE Security & Privacy*, *13(3)*, 80-83.

Turland, J., Coventry, L., Jeske, D., Briggs, P., & Van Moorsel, A. (2015). Nudging towards security: Developing an application for wireless network selection for android phones. Proceedings of the 2015 British HCI conference, ACM, pp. 193-201.

Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, *5(2)*, 207-232.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber

hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128,* 113-160.

Von Der Gracht, H. A. (2012). Consensus measurement in Delphi studies: review and implications for future quality assurance. *Technological forecasting and social change, 79(8),* 1525-1536.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security, 38,* 97-102.

Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards the future internet of things. In: Uckelmann, D., Harrison, M., Michahelles, D. (Eds.), Architecting the internet of things. Springer, Berlin (Germany), pp. 1-24.

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18(1),* 3-7.

## Supplementary Information

**Acknowledgements**

The authors would like to thank Professor Jeremy Watson for his leadership of PETRAS and the project grant.

**Funding Details**

This work was supported by the UK Engineering and Physical Sciences Research Council under Grant number EP/N02334X/1.

**Author Information**

NA, JB and CL contributed to the study while working as Senior Research Fellows/Research Fellows during employment at University College London (UCL), UK. SM is a Professor of Health Psychology and Director of the Centre for Behaviour Change at UCL (UK).

**Declarations of Interest Statements**

***Declarations of interest***

The authors declare that they have no conflicts of interest.

***Submission declaration and verification***

The authors declare that the work has not previously been published, it is not under consideration for publication elsewhere, and its publication has been approved by all authors and authorities where the work was carried out. If accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copy-right holder.

***Data Availability Statement***

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

## Supplementary Files

### Supplementary File 1 – Round One Qualitative Questionnaire

Welcome. You have been invited to take part in our expert consensus study on the Internet of Things. You will be asked to assess threats and behaviours in two contexts, the home environment and the work environment. Next we briefly define these contexts and provide examples for IoT applications in these contexts.

- Internet of Things home environments - This context refers to consumers' use of connected devices for personal use at home and on the go. This may include scenarios like the following examples:
    - Example 1: Home. Smart homes integrate multiple IoT devices and services providing users with the ability to control and adapt the status of their household manually or automatically. The smart home may offer many services to users including controlling the home with voice commands or from afar, recognising who is at the front door, learning household occupant preferences and communicating maintenance issues to the home owner (such as leaking pipes, broken boilers).
    - Example 2: Health. IoT health devices allows users to manage their wellbeing, fitness and health through wearable technology that can provide real time feedback to users. Other IoT healthcare devices can include those that aid patient treatment and adherence such as devices designed to help prescription dispensing, weighing scales and blood pressure and sugar monitors.
    - Example 3: Transport. The connected car may provide enhanced services to consumers by being able to communicate with parking spaces, provide real-time traffic information, safety and diagnostics, ability to connect with other household appliances, breakdowns services, wirelessly control devices in the home and communicate with other smart sensors within cities.
- Internet of Things work environments - Refers to situations in which IoT devices will enhance organisational productivity and efficiency. We will focus on contexts in which these IoT devices and environments specifically relate to employees and their behaviour. This may be in the following scenarios:
    - Example 4: Intelligent workplaces. Devices will work together to meet professional needs of different occupations such as smart devices giving

employees directions to you next meeting, connected products that have multiple functions (e.g. staff ID card also works as a payment system), connected environments (e.g. lighting systems and heating systems that crowdsource optimal temperatures and settings), and business intelligence (collecting and curating data, simplifying the data and creating actionable outputs for specific employees).

- Example 5: Workplace wearables. This includes devices that employees can wear as part of their job to enhance their performance such as devices that promote safer driving by detecting when employees are feeling drowsy.

Please note. By 'behaviour' we are referring to individual's actions or conduct. For example, weight loss is not a behaviour but increasing physical activity and reducing calories are examples of behaviours that may ultimately lead to weight loss. Cyber hygiene concerns the protective behaviours (security, privacy and safety) that end-users can perform to mitigate and/or recover from IoT threats.

The following are the open-ended questions to be presented to experts.

1. Before focusing on IoT threats and behaviours, we are interested in your thoughts on current end-user behaviour?
2. What do you think are the IoT security threats that end-users will need to take action against?
3. What do you think are the IoT privacy threats that end-users will need to take action against?
4. What do you think are the IoT safety threats that end-users will need to take action against?
5. How do you think these threats differ between the home and workplace context?
6. What protective behaviours do you think are most important to mitigate the IoT threats you identified?
7. Rank order the three protective behaviours you think will have the biggest impact if changed:
    a. Rank 1:
    b. Rank 2:
    c. Rank 3
8. Rank order the three protective behaviours you think will be easiest to implement:

   a. Rank 1:
   b. Rank 2:
   c. Rank 3

9. Rank order the three protective behaviours you think will have a “spill over” effect:
   a. Rank 1:
   b. Rank 2:
   c. Rank 3
10. Rank order the three protective behaviours you think will be easiest to measure:
   a. Rank 1:
   b. Rank 2:
   c. Rank 3
11. Of the behaviours you have identified, please choose three behaviours you think are most important:
   a. Rank 1:
   b. Rank 2:
   c. Rank 3
12. For the behaviours you have discussed, how do you think they may differ in the workplace?
13. What are the differences between conventional protective behaviours and IoT protective behaviours (if any)?
14. What do you think are they key problematic behaviours that may undermine protective efforts?
15. What do you think are the differences between end-users current problematic behaviours and IoT problematic behaviours?
16. How do you think problematic behaviours may differ between home and workplace?

## Supplementary File 2 – Round One Selection Process

**Table 1:** *Percentage of experts and online sources reporting protective behaviours during Delphi Round One which subsequently satisfied the selection criteria for inclusion in Delphi Round Two*

| IoT Protective Behaviour | | | Responses | |
|---|---|---|---|---|
| **Lifecycle** | **Domain** | **Sub-Domain** | **Experts Frequency (n = 32)** | **Online Advice Frequency (n = 15)** |
| **Pre-Purchase** | **N/A** | Buy and use product and services from reputable companies | 22% | 27% |
| | | Buy devices that can work within the cloud | 3% | 7% |
| | | Buy devices with security-focused platforms | 0% | 3% |
| | | Decide whether considered IoT device is ideal for its intended purpose | 0% | 20% |
| | | Minimise the number of different IoT device providers that you buy from | 3% | 0% |
| | | Research the security of the IoT device before purchasing | 9% | 27% |
| **Set-up & Maintenance** | **Credential Management** | Change the default passwords on devices, networks and services | 13% | 60% |
| | | Don't reuse your passwords on devices, networks and services | 6% | 27% |
| | | Don't share your passwords | 6% | 7% |
| | | Regularly change passwords on devices, networks and services | 9% | 7% |
| | | Set-up account lock-out following failed password attempts, where possible | 6% | 0% |
| | | Use a password manager application | 0% | 20% |
| | | Use multi-faceted/two-step authentication, where possible | 6% | 0% |
| | | Use strong passwords on devices, networks and services | 28% | 73% |
| | | Write down passwords if needed | 3% | 7% |
| | **Network Management** | Disable "Universal Plug and Play (UPnP)" on your router | 3% | 20% |
| | | Ensure that your Wi-Fi is secure to at least WPA2 level | 0% | 20% |
| | | Isolate IoT devices onto their own network | 6% | 47% |
| | | Limit the number of connected devices and disconnect devices that no longer need an active connection | 9% | 27% |
| | | Monitor network traffic on your router | 6% | 0% |
| | **Device Settings** | Modify the privacy and security settings of the device in line with your needs | 19% | 13% |
| | | Understand and learn the system configuration and settings | 9% | 27% |
| | **Privacy protections** | Limit or disable the amount of information that the devices shares across networks and services to the minimum necessary | 9% | 13% |
| | | Limit sharing of your personal information with devices | 19% | 0% |
| | | Read and understand the terms and conditions | 13% | 7% |
| | **Updating** | Install updates as soon as they become available | 0% | 33% |
| | | Keep your device updated | 28% | 40% |
| | | Select "automatically update" when possible | 0% | 27% |
| | | Set a schedule to check for updates if "automatic update" is not available | 0% | 40% |
| | **Other** | Enable encryption of communications and data, where possible | 19% | 7% |
| | | Keep your personal devices off the workplace network | 0% | 13% |
| | | Only use authorised software/services with your IoT devices | 6% | 0% |
| | | Read and familiarise yourself with the manufacturer's instructions during installation | 0% | 20% |
| | | Read articles about IoT security, safety and privacy issues | 6% | 0% |
| | | Use a strong firewall | 6% | 7% |
| | | Use online IoT scanners to check for vulnerabilities | 0% | 7% |
| **Disposal** | | Discard devices that have security weaknesses that can be fixed | 6% | 7% |
| | | Remove unsafe devices from the network | 9% | 13% |

**Table 2:** *Percentage of experts and online source reporting risk behaviours and threats during Delphi Round One which subsequently satisfied the selection criteria for inclusion in Delphi Round Two*

| Behaviour | Sub-Domain | Experts Frequency (n = 25) |
|---|---|---|
| **Risk Behaviour** | Choosing weak passwords | 24% |
| | Disabling security features | 12% |
| | Not changing the default password | 16% |
| | Not changing the default settings | 16% |
| | Not installing software updates | 16% |
| | Password re-use | 20% |
| | Placing convenience over security | 12% |
| | Sharing of too much personal data | 16% |
| | Visiting risky websites | 12% |
| **Threats** | Botnets | 12% |
| | Compromised control devices | 28% |
| | Compromised safety critical alerting devices | 60% |
| | Counterfeiting | 12% |
| | Data mining and harvesting | 24% |
| | Denial of service | 12% |
| | Eavesdropping | 36% |
| | Malware | 12% |
| | Man in the middle attacks | 12% |
| | Physical tampering of devices | 12% |
| | Social engineering | 12% |
| | Tracking users | 36% |