Refining the Blunt Instruments of Cybersecurity: A Framework to Coordinate Prevention and Preservation of Behaviours

Simon Parkin[1] and Yi Ting Chua[2]

[1] University College London, UK
[2] University of Cambridge, UK
s.parkin@ucl.ac.uk, yiting.chua@cl.cam.ac.uk

Abstract. Background. Cybersecurity controls are deployed to manage risks posed by malicious behaviours or systems. What is not often considered or articulated is how cybersecurity controls may impact legitimate users (often those whose use of a managed system needs to be protected, and preserved). This characterises the 'blunt' nature of many cybersecurity controls.
Aim. Here we present a synthesis of methods from cybercrime opportunity reduction and behaviour change.
Method. We illustrate the method and principles with a range of examples and a case study focusing on online abuse and social media controls, relating in turn to issues inherent in cyberbullying and tech-abuse.
Results. The framework describes a capacity to improve the precision of cybersecurity controls, identifying opportunities for risk owners to better protect legitimate users while simultaneously acting to prevent malicious activity in a managed system.
Conclusions. We describe capabilities for a novel approach to managing sociotechnical cyber-risk, which can be integrated into typical risk management processes, to allow for side-by-side consideration of efforts to prevent and preserve different behaviours in a system, by examining their shared determinants.

Keywords: risk management, cyber risk, sociotechnical security.

1 Introduction

Cybersecurity controls are deployed within a managed IT system, such as in a business or an online service platform, to manage cyber risks and address unknown or anticipated malicious behaviour. Implicit in common security and privacy risk management practices is that if a control is well-intentioned, it will not do any harm to those it is meant to protect. Cyber threats can impose a range of different harms upon legitimate users [3], however so can cybersecurity risk controls if not carefully considered [17]. This can result in e.g., legitimate users being removed from a system, or their activity being misclassified. Such *unintended harms* may be more severe for specific user groups who lack targeted support (such as the technical skills assumed to follow basic advice), or are inadvertently treated as malicious entities (e.g., by rules for identifying suspicious activity on a social media platform). To prevent these harms, we need a capacity to identify them in advance.

The potential for risk controls to harm legitimate users is pronounced in modern IT systems, as the *hyperconnectivity* they embody between individuals [52] means that malicious and legitimate activity in the same environment has some of the same observable behaviours and use of the same infrastructure (e.g., accessing an online account through the same interface). We must ensure that a candidate risk control does not impact existing activities and controls associated with legitimate users.

Many methods exist for analysing a whole system to discourage a malicious behaviour [19,20], or to promote positive behaviours [60], i.e., behaviours to encourage (whether they relate to security and privacy or not — Section 2). We consider the latter schools of science together, as a means to avoid 'blunt' controls which reduce malicious behaviours at the cost of legitimate behaviours. An example would be an automated detection system which blocks both malicious and legitimate users, or changing system features to stop an attack but making other benign activities difficult or impossible. This leads to approaches to address the sociotechnical *precision* of cybersecurity controls, to target only malicious or unwanted behaviours (Section 3). We note that to our knowledge, the interplay between these two groups of approaches has not been considered within or outside of cyber-risk management, though formative and disparate activities can be found.

We describe extensions to address gaps in existing risk management approaches, to explicitly consider user behaviour as an asset to protect; identifying shared determinant factors between negative and positive behaviours in a *sphere of interference*, and; the need to engage with stakeholders in the sociotechnical system in key risk management decisions. This acts as a foundation for a holistic cyber-risk management which is "user-friendly while abuser-unfriendly" [30]. We apply the novel approach to a case study on cyberbullying, where there are many cross-cutting concerns (Section 4). We close with discussion (Section 5) and directions for future work (Section 6).

2 Managing Security for an Ecosystem of Behaviours

With IT systems underpinning so much of what people do in their normal lives, legitimate users and malicious actors are using the same infrastructure and technologies, making it more difficult to distinguish between them. To address this, we explore the synthesis of crime science and crime prevention (Section 2.1), with behaviour change science (Section 2.2), alongside information security management standards (Section 2.3). This identifies gaps in existing cyber-risk approaches, and opportunities to refine the precision of sociotechnical security controls (Section 2.6), couched within existing cyber-risk management approaches.

2.1 Discouraging malicious security-related behaviours

Scholars have explored the applicability of existing crime prevention theoretical frameworks and approaches to the domain of cybercrime. Both social learning theory and general theory of crime have been applied to examine cybercrime, such as hacking behaviours [12,58,59], where both theories focus at the level of the individual. Other crime prevention approaches focus on the opportunity structures and immediate environment as causes of criminal acts. *Situational crime prevention (SCP)* has shown success in addressing numerous offline crimes such as burglary and car theft [19], and online crimes such as data breaches [24].

SCP is a framework of strategies aiming to reduce criminal opportunities arising from the immediate environment [18,19]. Rather than viewing crime as a result of criminal predispositions, it views crime as the result of one's deliberate choices and decisions [18], affected by a person's immediate situation and circumstances. This shapes the three inter-related features of *SCP*, being specificity of the crime, the immediate environment, and the individual's perception and decision to commit a malicious act [18,19]. Associated techniques fall under five categories, each containing five techniques: increasing efforts, increasing risks, reducing reward, reducing provocations, and removing excuses [19,25,75]. These *opportunity reduction techniques* target the potential components of criminal opportunities [19,21,25,75], affording precision in targeting malicious behaviour.

Routine Activity Theory (RAT) emphasises the circumstances around when crimes occur [23,38]. Its main proposition is that crime occurs as the convergence in space and time of a suitable target, a motivated offender, and the absence of a capable guardian [23,38]. This last element refers to any person or object with the potential capabilities to prevent the occurrence of a crime [23]. Although generally associated with formal guardians such as police officers, capable guardians can have informal roles, such as pedestrians on the street or security cameras in stores. *RAT* has been adapted to explain victimisation as a result of online lifestyle and routine behaviours, while conceptualising computer and cybersecurity features as effective guardians [15]. Here we focus on risk owners within a managed IT infrastructure as 'guardians' of legitimate users in a system, acting to reduce the opportunities and capacity to conduct malicious activity.

2.2 Encouraging positive security-related behaviours

A range of factors are critical to encouraging an individual to adopt a positive behaviour. The COM-B model [60] distills critical factors for promoting behaviour change, namely capability, opportunity, and motivation. The authors position these factors alongside complementary layers of intervention and policy activities (such as environment design). These then complement the broader range of levers found in situational crime prevention (Section 2.1); it also indicates that there is a shared environment where interventions to prevent and to promote behaviours may all be happening in the same place. Similarly, the 'B=MAP' behaviour change framework [39] encompasses the need for a combination of Motivation, Ability, and Prompt for new behaviours to form. Prompts have been explored for security elsewhere (in security advice for consumers [63]).

Clear [22] outlines principles necessary to position and sustain a good behaviour, and de-emphasise unwanted behaviours. The latter can include making a behaviour more difficult to accomplish, less visible, or less desirable. If risk controls are not targeted sufficiently, they may induce effects upon otherwise positive behaviours which mirror the same techniques used to break bad habits. Similarly, the Theory of Planned Behaviour (TPB) [4] highlights the importance of self-efficacy (a person's belief that they can enact a behaviour toward an intended outcome), which is critical for security-related behaviours [35]. Regarding controls themselves, if a behaviour is seen as undermined and unlikely to succeed, this reduces (positive) control beliefs.

Intervention Mapping [7], within the health domain, identifies relationships between critical factors for an intervention aimed at an 'at risk' group. The approach acknowledges that development and deployment of an intervention is a collaborative activity involving a variety of stakeholders. The approach identifies behavioural and environmental causes of problems, producing *determinants* of problem behaviours. The approach also advocates *"reframing problem behaviors and environmental causes of health problems as desirable behaviors and environmental outcomes"*. Subgroups are further differentiated through targeted performance objectives and determinants. Being precise is then framed as key to encouraging and sustaining good behaviours. These principles have been applied in targeting cybersecurity awareness initiatives [65].

Again looking to the health domain, the PRECEDE-PROCEED intervention framework [41] includes a PRECEDE phase, which diagnoses factors critical to an intervention, including behavioural and environmental factors. This phase includes identifying the activities of actors which can affect the environment. Here we develop an approach for cybersecurity for actors, such as cyber-risk owners, to engage in this kind of diagnosis. PRECEDE-PROCEED emphasises the development of more specific interventions to target a particular group and behaviour, including factors which promote or prevent a behaviour. Here we argue that the need for such precision should be emphasised similarly in the design of cybersecurity interventions, rather than *after* an intervention has been enacted as may be seen if they contribute to harms.

2.3 Risk management for systems of behaviours

We refer to *risk owners* as the stakeholders in an IT environment who have the authority and decision-making responsibility to enact changes to the cybersecurity apparatus within that environment (including technical and sociotechnical controls). This is aside from a risk owner potentially being the person assigned responsibility in an organisation. We refer to risk management literature aimed primarily at organisations, as it is indicative of how security-related behaviours may be managed and allows us to build on practices familiar to risk managers.

Various risk management approaches have hinted at issues tangential to our aims, albeit without directly addressing the linked impacts between efforts to *prevent* and *preserve* different IT-facilitated behaviours concurrently. ISO/IEC 27005:2011 ('Information security risk management') [53] explicitly includes 'Identification of consequences', though focusing on the consequences of a threat upon an asset, with no explicit examination of the impacts a control may have upon that asset. The broader ISO/IEC 31000:2018 'risk management' guidelines [13] acknowledge that risk management efforts may produce unintended consequences, noting that implementation of risk treatment plans ought to ensure that controls are effective when they are deployed, or otherwise that any risks they introduce are managed.

Related 'Risk management techniques' in ISO/IEC 31010:2009 [49] outline *consequence analysis*, to capture impacts including those affecting different objectives and different stakeholders. It is also advised to capture how consequences relate to the original objectives, and secondary consequences, with further consideration of *hazards*, including physical harm. The potential for knock-on impacts from managing one risk upon another risk are highlighted, but not further developed. The need to ensure a 'freedom from risk' is acknowledged in the digital domain within standards for software development (as in ISO 25010 [50]). Techniques exist in cyber-risk management standards which can minimise unintended harms to legitimate users, but are not being coordinated to do so.

The NIST 'Risk Management Framework for Information Systems and Organizations' standard [54] brings attention to "potential adverse effects on individuals", and that some capabilities must be upheld to meet stakeholder needs. Our framework addresses a need for *existing* security and non-security capabilities to escape impact from subsequent countermeasures. The OCTAVE risk management process [5] considers how a risk management strategy itself can impact 'exposed assets'. We argue that users and behaviours linked to known, permitted capabilities within a system should be explicitly regarded as assets to protect, echoing directions outlined by a successor to OCTAVE, OCTAVE Allegro [14].

2.4 Existing examples

The following are examples of where consideration of the interplay between malicious behaviours and legitimate user activities has resulted in precise targeting of negative outcomes while preserving positive behaviours.

- **Phishing reduction through token authentication.** Google employees were provided with two-factor authentication (2FA) tokens [57]. Rather than relying solely on training to avoid phishing attacks, this recognises that email links and service access can be typical in work, and that malicious/fake links etc. may be difficult to spot all of the time, making them difficult to separate.

By using physical tokens to enable system access, a ‘successful’ phishing attack does not gain enough credentials to compromise a system (nullifying the value of knowledge-based credentials). This also means that employees are not under pressure to identify malicious links themselves to avoid compromise at all cost, and as a result warp their treatment of legitimate emails.

- **‘Loan-phones’ during digital forensics activities.** When a personal phone is being analysed for evidence of domestic abuse, some police forces in the UK provide a temporary phone, while some may not (which can factor in grave consequences [10]). A temporary phone preserves a person’s capacity to reach their social support network or seek help. Here, a control to collect data of malicious activity (from smartphones) inadvertently removes the smartphone from its user; provision of loan phones reduces the impact to positive behaviours.
- **Socio-technical password controls.** There have been approaches in UK policy[3] to shift effort in managing passwords from end-users to background technical controls, so that legitimate users do not face the same difficulties that are created to dissuade malicious behaviour. For instance, system monitoring may be able to detect suspicious system activity and block access to legitimate login sites. 2FA tokens, as above, is a similar measure, reducing the heavy reliance on legitimate users to protect their passwords.

2.5 Related work

The SCENE framework [26] suggests to develop cybersecurity behaviour change options so that the most secure options are most accessible, ideally as ‘defaults’ (as applied for wi-fi selection [73]). Similar to behaviour change and crime reduction approaches, SCENE advocates co-creation of solutions with target audience and stakeholders. We posit that the available options for using IT securely may be reduced by efforts to reduce malicious activity.

Agrafiotis et al. describe a taxonomy of *cyber harms* [3] which may be observed in organizations. The taxonomy comprises five broad themes, including digital harm, and social and societal harm. The authors posit that analytical tools are necessary to reduce these harms, and as part of risk assessment. Similarly, Chua et al. [17] encourage risk managers to explore the potential for *unintended harms* to emerge as a result of their own risk controls. The authors’ framework emphasises the need to support vulnerable populations who may experience harms if risk controls work against them rather than for them. We identify factors which contribute to unintended harms, rather than consequences.

The Security Function Framework (SFF) [29] surfaces design considerations for sustainable crime reduction solutions, and creation of new products. Ekblom notes that malicious actors and their (potential) victims may have *script clashes* [32], with a need to design solutions to “favour the good guys”. Where a crime reduction solution has a *niche* [31] in how it relates to “other products, people

[3] “Password policy: updating your approach”: `https://www.ncsc.gov.uk/collection/passwords/updating-your-approach`

and places in the human, informational and material ecosystem", we pursue a similar notion of *precision*. As we consider user communities in IT ecosystems, this involves users, user behaviours, and infrastructure.

2.6 Synthesis of sociotechnical risk-related research

We have shown in the above analysis that activities to reduce behaviours are linked to activities to promote or sustain behaviours, arguably more so in hyperconnected IT systems. Risk management standards hint at the need to balance these efforts, but do not sufficiently articulate and address the needs to protect users and existing user behaviours. Both negative behaviour and positive behaviour change approaches iterate over an intervention to reach a *more precise solution*. Behaviours are regarded as the result of a combination of individual factors (motivations, personal beliefs, self-control), capabilities of the individual, behavioural factors, and environmental factors (opportunity, rewards and punishments). *Linkages* between definitions of positive and negative behaviours can then be identified, as a measure that acting on one can impact the other, creating what we refer to here as *interference*.

Techniques in both crime reduction and behaviour change both act to move from an undesirable behaviour to a new target behaviour. Risk management and crime reduction approaches focus on undoing negative behaviours, but given the interconnected nature of cyber-risks, what is missing is a consideration to protect existing positive behaviours while doing so.

When identifying determinants from the perspective of crime prevention, the first step is having a specific definition of a malicious behaviour, regardless of the level of determinants [19]. Small variations in malicious behaviour are the results of a combination of factors [19,23,25,38]. Specifying a malicious behaviour allows for more precise identification of determinants. Behaviour change approaches, such as Intervention Mapping, are similarly *specific in defining behaviours*.

We make a simplifying assumption that a risk owner is afforded more sight than any other stakeholder of candidate risk controls and their features. This means they can better develop an awareness of causal factors for user behaviours as defined in a control [69]. *Engagement with stakeholders* (including guardians managing offenders, targets, and places) is encouraged to reach effective solutions, in both crime reduction and positive behaviour change. We see in our Case Study (Section 4) examples of action taken by parents to protect their children online. Those managing or encouraging positive behaviours are best-placed to identify potential consequences. We then focus on those mechanisms under the view of a risk owner which can result in changes to other parts of the system (Section 3.1).

The identification and involvement of stakeholders in shaping controls appears somewhat open-ended in current risk management approaches. Risk management standards are generally quite detailed in determining how the actors and constituent elements in a system may be adversely affected by an incident or malicious activity, but this same rigour is not applied to the controls themselves. Where ISO 27005:2011 [53], for instance, refers to the 'scope and boundaries' for a risk control, the notion of 'boundaries' in cyber-risk management requires development in terms of how user needs are identified with stakeholders. Techniques may be adapted relating to guardianship in *RAT*, or crime preventers and promoters in the work of Paul Ekblom [31]. There needs to be greater *proactive effort to identify stakeholders* to avoid harms from deploying a risk control.

We argue that positive behaviours exhibited by legitimate users need to be an explicit part of cyber-risk assessment, but that there is a pronounced gap in existing cyber-risk management approaches, where *sociotechnical assets* are not directly considered despite being represented in systems as user profiles, behaviour data, and system management decisions/rules which act upon them. Risk management is at present centred around data and artefacts of value, but the behaviour of legitimate users is not directly considered. However, changes in how aspects of existing risk management approaches are emphasised can realise more holistic, user-centred outcomes. We address this in the next section, toward *sociotechnical risk management.* We also consider the shared language of mediations between preventative behaviour management and positive behaviour change in secured systems, as a means of moving beyond blunt instruments in cybersecurity.

3 Framework for Precision in Sociotechnical Controls

3.1 Prevention and preservation of behaviours

Risk controls in an IT environment potentially restrict behaviour, users, and infrastructure [17], in turn affecting actual user behaviour, through their representations in IT systems. A risk owner making decisions about IT-security and related technical systems is unlikely to have a direct view of what users are doing. Instead they have access to systems which record or prohibit particular activities on systems, as data. There is then a lack of explicit acknowledgement of the connections between what would normally be considered assets to protect, such as data and systems, and the legitimate user activities that use those assets.

For our purposes, this is directly addressed by adopting the mechanistic approach to cybersecurity described by Hatleback and Spring [44]. With this, a behaviour can be an *indexed entity*, as a file or data, but also exist as an activity in a system, producing a visible phenomenon. An example would be a 'delete' function which exists as rules, but can also be enacted as an activity which is run within the system.

A foundation for precision in sociotechnical security controls extends the definition of an asset to include indexed entities (Figure 1). This relates (positive and negative) real-world behaviours to identifiable data and systems which a cyber-risk owner imposes decisions upon. Critically, there is a feedback loop between System Assets and People — if there are rules about how data can be created in a system, these rules may restrict the activities of People. Examples include restrictions on credentials necessary to make a new account on a system, or checks for particular kinds of behaviour which are permitted.

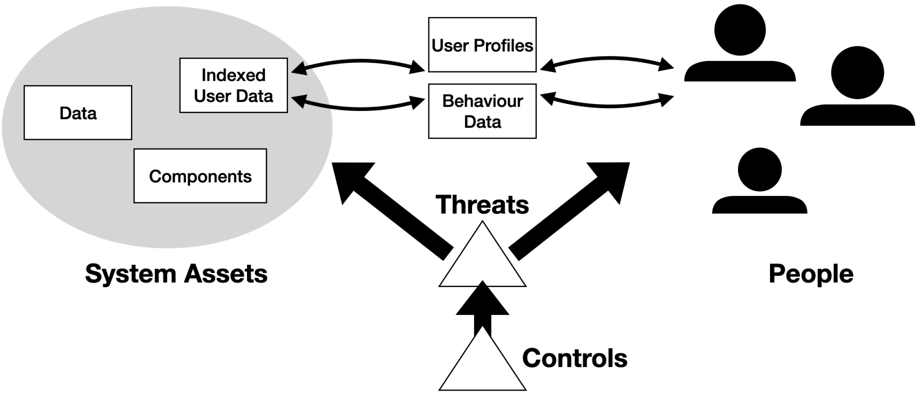

Fig. 1. Extending risk management artefacts to accommodate sociotechnical risk management. Individual People may interact with a system in such a way that User Profiles and Behaviour Data are generated and maintained. These are then Indexed User Data, generated as system activities alongside the behaviours of People using a system.

If we are able to represent behaviour as an indexed entity in a managed system, this leads to the challenge of coordinating two up-to-now distinct efforts. The first is the removal of negative/malicious behaviours from the system, e.g., inflammatory posts on social media. The second is maintaining positive behaviours already in the system, e.g., allowing users to share posts on social media. Where risk management often involves maintaining a *risk register* of top risks, a specific risk management activity is generally missing to address the second of these efforts, and record user behaviours which are active in the system and must be preserved. An example would be that a legitimate user from a particular geographic location should be able to make regular posts to a social media platform and share links if they would want to, but that malicious activity seeming to emerge from the same area, posting fake messages and sharing malicious links, ought to be stopped, as may happen in online romance scams [17]. The capacity to populate a (positive) *behaviour register* is needed, where this is a natural extension to existing risk management techniques, aligning with behaviour intervention approaches (Section 2.3).

3.2 Intersection of behaviours to prevent or preserve

As in Figure 2, we describe a method of sociotechnical cyber-risk management to coordinate refinement of precision in security controls. Existing (cyber)crime reduction techniques and behaviour change approaches amply describe how to manage individual behaviours. As a first step, we propose to consider the Capability, Opportunity, and Motivation of a behaviour [60], as common terminology from both domains, to allow for comparison between two sets of specific behaviours and allow for refinement of controls. For simplicity, a 'positive' behaviour can include continuing not to do a behaviour which is detrimental [40]. If

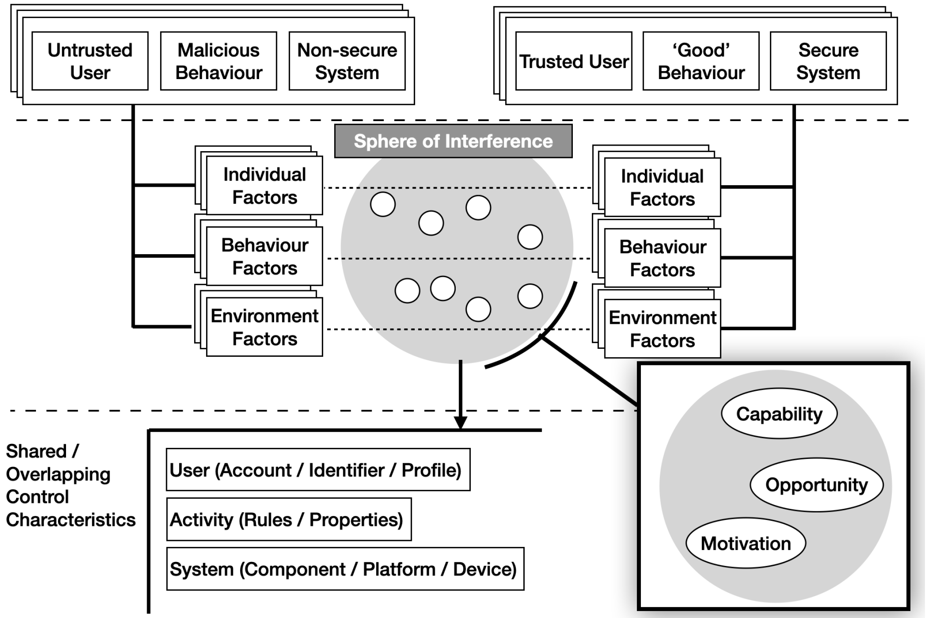

Fig. 2. Overview of proposed unison of negative and positive behaviours in a managed (cyber) system, and related controls.

separating legitimate and malicious behaviours is difficult, this indicates where *linkages* between them are strongest, and the need to unpick them more critical so as to avoid unintended harms to positive behaviours.

A further step is to identify sufficiently detailed definitions of User, User Behaviour, and Infrastructure, as these are elements familiar to a cyber risk owner, but which also influence the COM factors in behaviours (as evidenced by risk controls preventing malicious behaviours). The extended asset definition in Figure 1 supports this. An extended behaviour definition that relates to user behaviours also serves as a *trading zone* [69] between cyber-risk management, reduction of negative behaviours, and retention of positive user behaviours.

Crime reduction techniques (Section 2.1) are advocated here to identify negative behaviours, and in turn interact with risk management approaches (Section 2.3) to identify candidate controls. The behaviour change approaches in Section 2.2 are leveraged to identify positive behaviours to preserve. The latter requires a retrospective view of which behaviours are to be retained in the system, which is not exactly what behaviour change approaches do, but indicates a need to catalogue behaviours much like there can be a record of the technologies deployed in an IT environment.

3.3 Identifying lack of precision in risk controls

From prior analysis in Section 2, our method includes the following steps:

Step 1. Record behaviours in the system.

1A **Identify active behaviour reduction activities.** This requires a catalogue of (malicious) behaviours being actively targeted, $R_1 - R_N$. See both cybercrime reduction approaches in Section 2.1, and risk management approaches, Section 2.1.

1B **Identify active behaviours to be preserved**. This set, $P_1 - P_N$, includes behaviours being promoted as part of active intervention programmes. This requires communication with other stakeholders in the system, as in common behaviour change approaches, Section 2.2. In organisations, the extraction of permitted behaviours can begin with access control policies, computer fair use policies, and include discussions with team managers to understand regular work activities [55]. In IT environments more broadly, this requires discussions with user representatives and local community experts (as with responding to tech-abuse [62]).

1C **Identify candidate controls.** This identifies controls $C_1 - C_N$, and applies to managing both negative behaviours and protecting positive behaviours. Involving stakeholders will make this more tractable. Once conducted, assessments may be reusable, making it less demanding over time and akin to maintaining an ongoing *risk register*. Such a register would describe concerns to manage (left-side of Figure 2), and a *behaviour register* of existing behaviours to preserve (right-side of Figure 2). It may not be possible to confirm that all behaviours and associated controls in the system have been identified, but efforts to do so should be documented.

Step 2. Map connections between behaviours and system assets.

2A **Identify sociotechnical representations of behaviours.** For each Control C in $C_1 - C_N$, identify the Environment, or *cyberplace* [51]; the Behaviourial determinants, Individual factors, and related data representations as recorded in IT systems (the *indexed assets*) that it acts upon. User activities must translate to user or behaviour representations (data or rules, Figure 1), or system elements, for a cyber-risk manager to be able to work directly with the information. Behaviour change approaches emphasise that it is critical to involve stakeholders in identifying target behaviours.

2B **Map behaviour determinants to technical features.** This will relate the impacts of controls on Environment and Behaviour to the Individual. For specific behaviours and their candidate controls, map data and systems to COM-B properties [60]. This can, for instance, map Capabilities to rules for permitted activity, or account properties; map Opportunity to restrictions on account access (such as registration requirements, or rules for signalling malicious behaviour); map Motivation to assumptions about workload/effort around what users will need to do to have access to a service (including technical knowledge). Having an Opportunity facilitated in technology does not necessarily mean that it is easily accessible. For instance, target-hardening efforts may make a system less accessible to legitimate users. For this reason, a user having access to — and being present in — an IT environment should be managed as a conscious Control decision.

Step 3. Address linkages between negative and positive behaviours and/or controls. Controls are engineered mechanisms [44] — it may be assumed but is not always assured that a control precisely addresses only the entity or activity it is intended to act upon. This means there is scope to address linkages. Controls and Behaviours must both be assessed together in an iterative manner. If it is found that any mapping of COM-B features to user, activity, or system entities overlaps between the *negative* and *positive* sets, it should be assumed that there is a legitimate group of users which will be affected by a cyber-risk management control if it is deployed. For instance, specific access restrictions may be activated by particular device or account details, but these rules might affect legitimate users sharing the same traits. A stark example is when one US police force was prevented from rapidly registering temporary email addresses after a ransomware attack, as systems treated this as activity associated with a spam campaign [9]. Linkages would require *remediation* (see Section 3.4) to break, or record and compensate for, the shared dependency between positive and negative behaviours. The number of linkages is a basic indicator of potential harms and a lack of precision in the candidate control.

3.4 Managing for the precision of risk controls

If a control affects both positive and negative behaviours, there may be a need to *reconsider* it. This would involve searching for a candidate Control which does not act on shared determinants, but only on negative behaviour determinants. With adaptation, current risk management processes would accommodate this, including searching for existing solutions already available to the risk owner. This highlights the need to take a mechanistic approach to understanding the role of security-related technologies in real-world systems [69]. Precise approaches for achieving this must be developed, where existing risk management guidelines can be adapted to identify controls which appropriately address a risk, relative to other activities already active in the system.

If a Control is adaptable, it can be *refined* — this applies more so to Controls which can be configured in how they interact with People, such as detection rules for system/online behaviour. We make an assumption that cybersecurity controls are generally deployed without an initial check of whether they carry the kind of *residual risk* which can result in *unintended harms*. There must be agreement with stakeholders that a control adequately minimises or avoids harms. If there is an expectation of potential harms to legitimate users — where negative and positive behaviour determinants interact — there may be a choice to *compensate* for the harm, and accept a candidate control but with additional compensatory measures. This may happen if a control is deemed necessary but expected to be short-lived (such as to address an emergent security threat). Refinements may be realised through e.g., configuration of data processing rules, policies for user identification and verification, user behaviour detection rules, and device detection and management rules.

Any lack of knowledge or expectations around the knock-on effects of a cybersecurity control should be logged as a residual risk ('unidentified risk' as in 27005:2011 [53]). This may be the case if a control is relatively novel. This relates to *ongoing attentiveness* to making systems work together (Section 5), realised most readily by measuring the performance of the system. The process should include input from non-security stakeholders, where their perception of consequences of cyber-risks must be considered [3]. Existing risk management approaches already advocate this, but not necessarily the residual risk of controls for legitimate users, or how to identify this particular kind of risk.

4 Use Case — Online Abuse Controls for Social Media

Here we consider a potential application of the framework to a real-world environment, specifically use of online social media platforms and prevention of online abuse. This is a domain in which platform operators have needed to iterate controls for security and privacy, to ensure that a range of different legitimate users can use social media with confidence, while at the same time identifying and preventing malicious activity. Online abuse continues to be an issue as technology and the Internet are interleaved with our everyday lives. Some common behaviours considered as online abuse include trolling, online harassment, stalking, bullying, and online threats, to name a few [43,47,71]. The increased use of social media platforms (*SMPs*) like Facebook and Twitter allow for continuous contact between offenders and targets without regard for physical and temporal distance [47]. This constitutes negative behaviour to be prevented on SMPs.

To address the negative behavior, SMPs introduce controls to minimise its occurrence and impacts on users (e.g. [36,68,72]). The necessity of such controls is increasing as the use of SMPs continue to grow among teenagers and adults[64] and is encouraged for their beneficial effects. Ellison and colleagues [34] found Facebook use among college students positively correlated with social capital that provides individuals with access to resources and information. In this instance, there are potentially two positive behaviours to be preserved: encouraging continued use of SMPs while lowering the risks of users becoming targets as they converge with offenders in the same online social space (e.g., online trolls). Personal privacy controls are then realised in part through security controls which maintain a safe environment which users can trust.

4.1 Factors in positive and negative behaviours

One factor affecting the utilisation of controls is the 'privacy paradox', where there is a discrepancy between expressed privacy concerns and privacy-related behaviours [6]. For instance, users reported utilizing features such as friends-only content accessibility, but at the same time accepting large numbers of friend requests from individuals who may not be seen as friends beyond the context of the SMP [28]. Another factor is the possible overlap between offenders and targets in cyberbullying and cyber-interpersonal violence [16,74]. This overlap is exacerbated by a reliance on users to be proactive and take action.

Current literature establishes a range of factors contributing to the rise of online abusive behaviors. Factors to consider at the individual level include pro-victim attitudes [33], perceptions of norms and injustice [11], and the contexts of exchanges [11,74]. Other relevant factors of cyberbullying relate to features of cyberspace, such as the anonymity and distance between users which can result in a sense of impunity and deindividuation; this can lead to adoption of online aggressive behaviours [43,46,66]. The nature of online media also means that users are removed from direct confrontation or consequence for their own behaviours [46,66]. Another feature is the scalability of the Internet, which allows multiple individuals to participate simultaneously in bullying behaviours [46].

There is some evidence supporting the effectiveness of these controls. Younger users of SMPs tend to be more proactive in adopting existing controls and settings to manage accessibility [2,6,27,28,56]. A comprehensive review on cyberbullying also found that blocking cyberbullies is among the most common strategies used and recommended among children and adolescents [2,42]. Some factors affecting the effectiveness of existing controls, especially privacy controls, are users' engagement, proactivity toward privacy, and technical skills [6,8]. These must be balanced with users' aims to communicate with others, potentially opportunistically or openly (as can be the case on online SMPs). This can require approachable means for finding other users on the same SMP, reaching others with messages they potentially were not expecting, and be able to tune interests to define the messages which are received from other accounts. In terms of security and privacy, this would require a blend of controls.

4.2 Risk controls

We acknowledge here that such an analysis looks at features and controls which have been deployed, rather than the design process behind them. Nonetheless, to combat the above issues, various SMPs have introduced controls to counter online abuse. There is the use of privacy settings and controls that allow account holders to manage accessibility to content via blocking or filtering [36,68,72]. Facebook later introduced the "friend list" feature to dictate the types of content each list has access to [37]. Snapchat provides more detailed description on controls, such as "Who can view my Story" and "Who can contact me" [68].

Another type of control is the introduction of clear community rules. The Snapchat community guidelines explicitly prohibit harassment, bullying, impersonation or violence, and encourage account holders to report these behaviours [67]. In the guideline, the SMPs listed punishments of different severity, from the removal of content, to termination of account, to the possibility of activity being reported to law enforcement agencies [67].

In some cases, the platforms attempt to include other stakeholders in their controls. Snapchat encourages parents to help adolescents in managing their accounts [68]. Parents have also advised their children to control privacy via the inclusion of false information [27].

4.3 Refining risk controls

In general, these controls address different COM-B characteristics that affect both behaviours that we wish to preserve (i.e., use of trustworthy and mainstream online SMPs) and prevent (i.e., online abuse). First, there is an inherent source of interference in the nature of the environment and users' motivations. The primary purposes for using SMPs include expressing one's identity digitally, maintaining and enhancing existing offline and online relationships, and creating new social relationships [76]. To do so, all users, both legitimate and malicious, are required to share some degree of information such as names and email addresses [70,76]. These requirements, along with the small to moderate effects between privacy concerns and users' utilization of privacy controls [6,8,28,56], suggest an increase in opportunities for malicious behaviours as the existing controls do not directly align with legitimate behaviours.

This raises the need for security controls to be in place to contribute to an environment which allows legitimate users to interact with other users, while also not preventing them from accessing the platform. The accessibility of personal controls for both privacy and security is also part of this need. Complications arise in the tension that stems from differences in the dynamics of online and offline social relationships. Online SMPs tend to oversimplify social ties into friends and not-friends [76]. Such dichotomous definitions do not always reflect the fluidity of social relationships in the offline world, adding to the effort required to maintain online privacy. In addition, users of online SMPs assign different value to different types of personal and sensitive information in cyberspace [1,2,56,70]. Variations in value assignment can interfere with perceptions of risks and opportunities, in turn affecting users' utilization of existing controls.

These studies highlight possible sources of interference between users' needs of SMPs and controls introduced on SMPs to protect them from harms. What is also highlighted are the potentially subtle ways in which well-intentioned controls may impact legitimate users. Both sources of interference suggest a need for proactive consideration of legitimate behaviours in the design of the controls, to limit misuse or ignorance of these controls. Risk managers need to have some level of understanding on the issue to better minimise the mismatch between expectations and outcomes, which result in the displacement of users to other platforms that provide a stronger sense of agency via easy-to-use privacy controls [2], or the reliance on alternative options [48].

5 Discussion

Our framework combines existing capabilities across disciplines, highlighting where adjustments can better manage sociotechnical risks. For instance, an existing risk register can be used, but locating existing positive behaviours may require concerted effort. This requires knowing what is happening in the system which has positive effects. Some positive behaviours may enter the system though not be the result of a specific intervention. This can require communication with specific stakeholders such as HR departments, user advocacy groups, etc. This is nonetheless more tractable than determining where users have been 'forgotten' or removed by risk controls [17], should a harmful control be deployed.

A risk owner may not be willing — or able — to Reconsider or Refine a control (Section 3.4). At an extreme, they may act to retain ignorance of potential harms emerging from a cybersecurity control, as 'organised irresponsibility' [3]. This introduces a different risk, of assuming that a control will not have impacts for legitimate users (which undermines security assurances), or that users will be able to manage any impacts transferred to them. This would be a form of Risk Acceptance, which relative to unintended harms would be *imposed acceptance* on users — in a hyper-connected system, users are impacted by a choice to do nothing about a risk. Even seemingly negligible costs to an individual user can collectively result in huge burdens for a user community in a larger system [45].

We propose a goal of a risk management methodology which combines prevention and preservation of behaviours to avoid linkages between them. This would bolster what Molotch [61] advocates, to *"add to rather than subtract from our well-being."*, by providing secure IT environments which are accessible to intended, legitimate users. Molotch also advocates *ongoing attentiveness* to interacting opportunities and constraints, which here would be regular oversight and dialogue with stakeholders (where at present, security guidelines signpost seemingly few points at which to engage parties with localised knowledge of user needs). We make the following initial recommendations for moving practice toward more precise sociotechnical cyber-risk controls:

- **Extend the definition of digital assets to include user *activities*.** In cyber-risk management processes, go beyond only considering data and components involved in activities within risk registers, to include representations of user behaviour. OCTAVE Allegro [14] advocates similar initiatives.
- **Measure the precision of controls.** This requires understanding of how a lack of precision — and consequent unintended impacts upon legitimate users — manifest in a system. A simple measure is the number of overlapping factors between controls to reduce behaviours and controls to promote behaviours in the same system (e.g., both legitimate activities and phishing attacks exploit hyperlinks).
- **Develop control portfolios to accommodate precision**. There must be capacity to tailor controls to match the specificity of negative behaviour controls and features which facilitate positive behaviours. The work of Hatleback and Spring [44], and Chua et al. [17], are steps toward shared terminology to navigate between prevention and preservation of behaviours.

For researchers in this space, aligning behavioural determinants and defining factors with system-level representations is non-trivial; here we proposed to translate these into elements of the COM-B model [60] and on into system representations (Section 3.3), but more specialised methods could be developed for this purpose, tangential to existing risk management approaches. Connections between crime prevention and behaviour change science as relate to cybersecurity can be considered further, including how these activities interact with each other within a sociotechnical system. Identifying how to improve risk controls to reduce impacts upon legitimate users is another area of potential future work — here we represent this through the dynamic between Behaviours and Controls, where novel design approaches can be developed.

6 Conclusion

We describe a framework for considering the concurrent prevention and promotion of different behaviours at the same time. This framework is intended to leverage existing risk management techniques familiar to practitioners, while also combining approaches from both (cyber)crime reduction and behaviour change techniques. We find that the definition of assets for risk management needs to be extended to explicitly include representations of user behaviour; the role of stakeholders is potentially underplayed in cyber-risk management standards, when their input is critical in collating legitimate behaviours to protect within an IT environment, and; that more must be done to measure unintended harms upon legitimate users and develop a capacity to configure candidate controls with a precision to avoid linkages to protected user behaviours.

As future work, we will explore the notion of sociotechnical precision in cybersecurity and cyber-risk management, with a real-world environment and related stakeholders. This will inform how behaviour and control refinement may operate in practice, with concrete challenges and discernible vulnerable populations. Future work will also explore how existing risk management standards can be adapted and extended to approach sociotechnical precision, while also retaining techniques familiar to the practitioner community.

References

1. Acquisti, A., Gross, R.: Imagined communities: Awareness, information sharing, and privacy on the Facebook. In: International workshop on privacy enhancing technologies. pp. 36–58. Springer (2006)
2. Adorjan, M., Ricciardelli, R.: A new privacy paradox? youth agentic practices of privacy management despite "nothing to hide" online. Canadian Review of Sociology **56**(1), 8–29 (2019)
3. Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T., Upton, D.M.: Cyber harm: concepts, taxonomy and measurement. Saïd Business School WP **23** (2016)
4. Ajzen, I., et al.: The theory of planned behavior. Organizational behavior and human decision processes **50**(2), 179–211 (1991)

5. Alberts, C., Behrens, S., Pethia, R., Wilson, W.: Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework, version 1.0. Tech. Rep. CMU/SEI-99-TR-017, Software Engineering Institute, Carnegie Mellon University (1999)
6. Barnes, S.B.: A privacy paradox: Social networking in the United States. First Monday **11**(9) (2006)
7. Bartholomew, L.K., Parcel, G.S., Kok, G.: Intervention mapping: a process for developing theory and evidence-based health education programs. Health Education & Behavior **25**(5), 545–563 (1998)
8. Baruh, L., Secinti, E., Cemalcilar, Z.: Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication **67**(1), 26–53 (2017)
9. BBC News: Google thwarts Baltimore ransomware fightback (2019), `https://www.bbc.co.uk/news/technology-48380662`, accessed: 15th September 2020
10. BBC News: Katrina O'Hara murder: Coroner recommends phone access changes (2020), `https://www.bbc.co.uk/news/uk-england-dorset-51557476`, accessed: 13th July 2020
11. Blackwell, L., Chen, T., Schoenebeck, S., Lampe, C.: When online harassment is perceived as justified. In: Twelfth International AAAI Conference on Web and Social Media (2018)
12. Bossler, A.M., Burruss, G.W.: The general theory of crime and computer hacking: Low self-control hackers? In: Cyber Crime: Concepts, Methodologies, Tools and Applications, pp. 1499–1527. IGI Global (2012)
13. BS, ISO: BS ISO 31000:2018 — Risk management — Guidelines. BS ISO (2018)
14. Caralli, R., Stevens, J., Young, L., Wilson, W.: Introducing octave allegro: Improving the information security risk assessment process. Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University (2007)
15. Choi, K.S.: Computer crime victimization and integrated theory: An empirical assessment. International Journal of Cyber Criminology **2**(1) (2008)
16. Choi, K.S., Lee, J.R.: Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. Computers in Human Behavior **73**, 394–402 (2017)
17. Chua, Y.T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G., Hutchings, A.: Identifying unintended harms of cybersecurity countermeasures. In: 2019 APWG Symposium on Electronic Crime Research (eCrime). pp. 1–15. IEEE (2019)
18. Clarke, R.V.: Situational crime prevention: Its theoretical basis and practical scope. Crime and Justice **4**, 225–256 (1983)
19. Clarke, R.V.: Situational crime prevention: Successful case studies. Albany, NY: Harrow and Heston Publishers (1997)
20. Clarke, R.V., Cornish, D.: Modelling offenders' decisions: a framework for policy and research'in tonry, m and morris, n. Crime and Justice: An Annual Review of Research **6** (1985)
21. Clarke, R.V., Homel, R.: A revised classification of situational crime prevention techniques. In: Lab, S.P. (ed.) Crime Prevention at a Crossroads, pp. 17–27. Anderson Publishing Co., Ohio (1997)
22. Clear, J.: Atomic habits: An easy & proven way to build good habits & break bad ones. Penguin (2018)
23. Cohen, L.E., Felson, M.: Social change and crime rate trends: A routine activity approach. American Sociological Review pp. 588–608 (1979)
24. Collins, J.D., Sainato, V.A., Khey, D.N.: Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. International Journal of Cyber Criminology **5**(1) (2011)

25. Cornish, D.B., Clarke, R.V.: Opportunities, precipitators and criminal decisions: A reply to wortley's critique of situational crime prevention. Crime Prevention Studies **16**, 41–96 (2003)
26. Coventry, L., Briggs, P., Jeske, D., van Moorsel, A.: SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In: International conference of design, user experience, and usability. pp. 229–239. Springer (2014)
27. Davis, K., James, C.: Tweens' conceptions of privacy online: implications for educators. Learning, Media and Technology **38**(1), 4–25 (2013)
28. Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication **15**(1), 83–108 (2009)
29. Ekblom, P.: The security function framework. In: Ekblom, P. (ed.) Design against crime: Crime proofing everyday products, chap. 2, pp. 9–36. Lynne Rienner Publishers (2012)
30. Ekblom, P.: Crime prevention through product design. Handbook of Crime Prevention and Community Safety. Abingdon: Taylor & Francis pp. 207–233 (2017)
31. Ekblom, P.: Technology, opportunity, crime and crime prevention: current and evolutionary perspectives. In: Crime Prevention in the 21st Century, pp. 319–343. Springer (2017)
32. Ekblom, P., Gill, M.: Rewriting the script: Cross-disciplinary exploration and conceptual consolidation of the procedural analysis of crime. European Journal on Criminal Policy and Research **22**(2), 319–339 (2016)
33. Elledge, L.C., Williford, A., Boulton, A.J., DePaolis, K.J., Little, T.D., Salmivalli, C.: Individual and contextual predictors of cyberbullying: The influence of children's provictim attitudes and teachers' ability to intervene. Journal of Youth and Adolescence **42**(5), 698–710 (2013)
34. Ellison, N.B., Steinfield, C., Lampe, C.: The benefits of Facebook "friends:" social capital and college students' use of online social network sites. Journal of Computer-Mediated Communication **12**(4), 1143–1168 (2007)
35. European Union Agency for Cybersecurity (ENISA): Cybersecurity culture guidelines: Behavioural aspects of cybersecurity (2018), `https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity`
36. Facebook: Abuse resources (2020), `https://www.facebook.com/help/726709730764837/?helpref=hc_fnav`, accessed: 10.09.2020
37. Facebook: Friend lists | Facebook Help Centre (2020), `https://www.facebook.com/help/204604196335128`, accessed: 08.12.2019
38. Felson, M., Cohen, L.E.: Human ecology and crime: A routine activity approach. Human Ecology **8**(4), 389–406 (1980)
39. Fogg, B.J.: Tiny habits: The small changes that change everything. Houghton Mifflin Harcourt (2019)
40. Fogg, B.J., Hreha, J.: Behavior wizard: a method for matching target behaviors with solutions. In: International Conference on Persuasive Technology. pp. 117–131. Springer (2010)
41. Green, L.W.: Toward cost-benefit evaluations of health education: Some concepts, methods, and examples. Health Education Monographs **2**(1_suppl), 34–64 (1974)
42. Hamm, M.P., Newton, A.S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S.D., Hartling, L.: Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. JAMA pediatrics **169**(8), 770–777 (2015)

43. Hardaker, C.: Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. Journal of Politeness Research **6**(2), 215–242 (2010)
44. Hatleback, E.N., Spring, J.M.: A refinement to the general mechanistic account. European Journal for Philosophy of Science **9**(2), 19 (2019)
45. Herley, C.: So long, and no thanks for the externalities: The rational rejection of security advice by users. In: Proceedings of the 2009 workshop on New Security Paradigms Workshop. pp. 133–144 (2009)
46. Hinduja, S., Patchin, J.: Cyberbullying: Identification, prevention, & response. Cyberbullying Research Center (2018)
47. Holt, T.J., Bossler, A.M.: An assessment of the current state of cybercrime scholarship. Deviant Behavior **35**(1), 20–40 (2014)
48. Househ, M., Borycki, E., Kushniruk, A.: Empowering patients through social media: the benefits and challenges. Health Informatics Journal **20**(1), 50–58 (2014)
49. IEC, ISO: 31010: 2009 risk management — risk assessment techniques. doi.org/10.3403/30183975 (2009)
50. IEC, ISO: BS ISO/IEC 25010:2011 - Systems and software engineering. Systems and software quality requirements and evaluation (SQuaRE). System and software quality models. IEC, ISO (2011)
51. Ife, C.C., Davies, T., Murdoch, S.J., Stringhini, G.: Bridging information security and environmental criminology research to better mitigate cybercrime. arXiv preprint arXiv:1910.06380 (2019)
52. Islam, T., Becker, I., Posner, R., Ekblom, P., McGuire, M., Borrion, H., Li, S.: A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems. In: International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications. pp. 277–293. Springer (2019)
53. ISO, IEC: IEC 27005: 2011 (en) information technology–security techniques–information security risk management. ISO/IEC (2011)
54. Joint Task Force: Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (final public draft) (sp 800-37 rev. 2). Tech. rep., National Institute of Standards and Technology (2018)
55. Kirlappos, I., Parkin, S., Sasse, M.: Learning from "shadow security": Why understanding non-compliant behaviors provides the basis for effective security. In: USEC '14 Workshop on Usable Security. pp. 1–10 (2014)
56. Kokolakis, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security **64**, 122–134 (2017)
57. Krebs, B.: Google: Security keys neutralized employee phishing (2018), `https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/`, accessed: 13th July 2020
58. Lee, J.R., Holt, T.J.: Assessing the factors associated with the detection of juvenile hacking behaviors. Frontiers in Psychology **11**, 840 (2020)
59. Marcum, C.D., Higgins, G.E., Ricketts, M.L., Wolfe, S.E.: Hacking in high school: Cybercrime perpetration by juveniles. Deviant Behavior **35**(7), 581–591 (2014)
60. Michie, S., Atkins, L., West, R.: The behaviour change wheel. A guide to designing interventions. 1st ed. Great Britain: Silverback Publishing pp. 1003–1010 (2014)
61. Molotch, H.L.: Against security : how we go wrong at airports, subways, and other sites of ambiguous danger. Princeton University Press (2014)

62. Parkin, S., Patel, T., Lopez-Neira, I., Tanczer, L.: Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. In: Proceedings of the New Security Paradigms Workshop (NSPW '19). ACM (2019)
63. Parkin, S., Redmiles, E.M., Coventry, L., Sasse, M.A.: Security when it is welcome: Exploring device purchase as an opportune moment for security behavior change. In: Proceedings of the Workshop on Usable Security and Privacy (USEC'19). Internet Society (2019)
64. Pew Research Center: Demographics of social media users and adopters in the United States (2019), https://www.pewresearch.org/internet/fact-sheet/social-media/
65. Renaud, K., Warkentin, M.: Using intervention mapping to breach the cyber-defense deficit. In: 12th Annual Symposium on Information Assurance (ASIA'17) June. pp. 7–8 (2017)
66. Sambaraju, R., McVittie, C.: Examining abuse in online media. Social and Personality Psychology Compass **14**(3), e12521 (2020)
67. Snapchat: Community guidelines (2020), https://www.snap.com/en-US/community-guidelines
68. Snapchat: Privacy settings (2020), https://support.snapchat.com/en-GB/article/privacy-settings2, accessed: 07.03.2020
69. Spring, J.M., Moore, T., Pym, D.: Practicing a science of security: A philosophy of science perspective. In: Proceedings of the 2017 New Security Paradigms Workshop. NSPW 2017, ACM (2017)
70. Taddicken, M.: The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. Journal of Computer-Mediated Communication **19**(2), 248–273 (2014)
71. The Crown Prosecution Service: Cyber/online crime (2020), https://www.cps.gov.uk/cyber-online-crime, accessed: 07.03.2020
72. TikTok: Safety center (2020), https://www.tiktok.com/safety/resources/anti-bully?lang=en, accessed: 07.03.2020
73. Turland, J., Coventry, L., Jeske, D., Briggs, P., van Moorsel, A.: Nudging towards security: Developing an application for wireless network selection for android phones. In: Proceedings of the 2015 British HCI conference. pp. 193–201 (2015)
74. Whittaker, E., Kowalski, R.M.: Cyberbullying via social media. Journal of School Violence **14**(1), 11–29 (2015)
75. Wortley, R.: A classification of techniques for controlling situational precipitators of crime. Security Journal **14**(4), 63–82 (2001)
76. Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and security for online social networks: challenges and opportunities. IEEE network **24**(4), 13–18 (2010)