Fostering a Cybersecurity Mindset

Professor William H. Dutton

Global Cyber Security Capacity Centre, University of Oxford and
The Quello Center, Michigan State University

In a conversation at a workshop on cybersecurity, Alastair Cook, Director of Critical Insight Security Ltd, argued that ‘the challenges in this area required a ‘security mindset’ among Internet users, security professionals and the organisations offering services.’ Research has explored attitudes of Internet users toward cybersecurity, as well as their security related practices. However, the concept of a ‘security mindset’ is a relatively under-researched idea, and one that could represent a subtle but important shift away from more common approaches to security, as well as to more user-orientated research on security attitudes or practices. This paper explores the promise of this conceptualization, and suggests some clarifications that could help progress this idea.

Is the idea of a mindset indeed a significant shift in thinking about cybersecurity? Can the concept of a security mindset be conceptually defined and empirically operationalized, or is it also a more qualitative shift to a sensitizing concept that captures a complex set of concrete habits, values and attitudes of Internet users? In either case, would it be a positive direction for guiding policy and practice? If so, how could this be accomplished? What are the policy implications of efforts to foster a security mindset? Might there be risks to fostering such a security mindset?

---

1 Bill Dutton is Director of the Quello Center at Michigan State University’s College of Communication Arts & Sciences where he is the Quello Professor of Media and Information Policy, and a Co-Principal of the Global CyberSecurity Capacity Centre. This working paper began while he was Professor of Internet Studies at the Oxford Internet Institute at the University of Oxford.

2 This is paraphrasing Alastair Cook’s comments at a workshop on 19 June 2014, with his permission.

3 Bruce Scheier has used this concept in a blog post, see: https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html
An analogy might be useful before I try to define the concept more precisely, such as by distinguishing this concept from related issues such as cybersafety. Better analogies might be suggested, but the example of bike security comes immediately to mind, having lived in Oxford for over a decade.

While living in Oxford, and biking to work, I would argue that nearly all bike riders in this city have adopted a security mindset. They do not think about whether or not to buy a lock, or whether or not to lock their bike when they leave it. They just do these things as a matter of course. It is a habit, yes, but also a mindset in that those purchasing or riding a bike have incorporated a set of assumptions that eliminate the need to move through a set of decisions on each particular occasion. They simply follow a course dictated by their security mindset.

Security provides a context to other decisions about other things. A person might even buy an older or less attractive bike in order to reduce the risk of it being stolen.

Moreover, it is a framework arising from the bottom up, rather than from the top down. For example, a bike lock is not part of the bike, or a required purchase, but something most users would incorporate with the purchase of a bike. The lock is viewed as part and parcel of the bike.

As it is bottom up, it is subject to broad social support by fellow bike owners. All riders lock their bike, and would question anyone who did not. Everyone can advise others on ways to secure their bikes. Buying a lock is not viewed as odd, but as normal. Not buying a lock would be viewed as silly by other bike riders, but not required by law, nor built into the bike itself.

In contrast, bike safety versus security might be less of a mindset in that you can see more variation among bike riders. Some equip themselves with a helmet, reflective clothing, and others do not. Riders might reflect on whether or not to use a helmet, depending on where they are riding and what they are wearing. It might be a mindset for some, but it is less universal and more flexible.

So – what is in a mindset? A mindset suggests a way of thinking about a matter of significance. It is a firm – not a fleeting or ephemeral perspective or framework for thinking about other things.
It is similar to a practice that is so routinized that it is almost automatic. It shapes choices about other matters. A security mindset might drive decisions about other aspects of Internet use. It arises from the interaction of peers – bottom up – rather than from sanctions or directions from above. In line with this, it is supported socially, such as through social pressure from friends and fellow users.

It is immediately apparent that a mindset is not a dichotomous state. You have it or you don’t. For example, a security mindset might be exaggerated in ways that would be dysfunctional. Some Information Technology Officers at many universities, for example, have become known for putting security above all or most other considerations. In my own experience, this can be taken to a fault and lead to poor decisions, such as postponing the adoption of wireless Internet access by many universities because it was viewed as insecure. The flip side of this is the reputed disregard of security or the absence of a security mindset by many Internet users, who fail to take minimal precautions in their computing practices, such as protecting passwords.

These two extreme examples suggest that a security mindset can error on either being set too high or low, exaggerating or under-estimating threats. In everyday life, television has been blamed for generating a ‘culture of fear’ that leads people to change their behaviour, such as not going out on the streets, when they actually have a very low probability of risk (Glassner 1999). Therefore, in fostering a security mindset, it is critical not to foster a culture of fear. In fact, a security mindset is a potentially valuable alternative to a culture of fear.

The example also suggests that the high cybersecurity mindset of the IT officer might be a functionally rational response to the perceived lack of a security mindset by too many users. If users lack a security mindset, in the eyes of the IT Officer, it could be up to them to protect the institution. Not only might the IT expert and user have different levels of focus on security, but their respective roles are a major issue among cyber-security researchers (Sasse 2014). Table 1 compares two ideal types (a expert-centric versus a user-centric) with the idea of a security mindset to illustrate the differences.
Table 1. A Mindset Perspective Compared to

<table>
<thead>
<tr>
<th>Ideal Types</th>
<th>Expert</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional Expert-Centric</td>
<td>Expert Controls, but Users Assigned Responsibilities</td>
<td>Users Blamed for Not Following Good Practice</td>
</tr>
<tr>
<td>Perspective</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-Centric Perspective</td>
<td>Experts Shoulder Key Responsibilities</td>
<td>Users Freed to Pursue Instrumental Aims, Not Required to Become Security Experts</td>
</tr>
<tr>
<td>Security Mindset</td>
<td>Experts Focus on Experts focus on Identifying and Addressing New Problems</td>
<td>Users Have Routinized Users Follow Secure Practices, enabling a focus on Instrumental Goals</td>
</tr>
</tbody>
</table>

However, it is unclear that the experts in IT can continue to protect institutions and the public, given the nature of the Internet and Web and social media, which will grow further with the rise of the Internet of Things (IoT). As Alastair Cook put it:

“If you ask an IT security person [expert] if they have a "security mindset", they will undoubtedly confirm that they have. They have been trained to have this "IT security mindset". However, this is narrower and too prescriptive a mindset for dealing with the spectrum of systems-of-systems risks that we should be adjusting to now.”

Clearly, the larger public of Internet users might need to be enrolled into a security mindset. The IT security officers will be less significant, making a mindset more relevant to a larger public. “[A security mindset] should be more accessible as technical understanding and technical measures become less significant in the management of security (Cook 2014).”

Previous research on the social aspects of cybersecurity has not focused on the notion of a mindset.4 The more traditional approach is to rely more heavily on security experts in industry

---

4 An overview of research is provided by Coventry et al (2014).
and organizations. For the purpose of contrasting this approach, it might be called ‘out of sight, out of mind’.

From this ‘out of mind’ perspective, the user is not well equipped to deal directly with security issues, nor is it appropriate to strap users with responsibility for security, as they are best focused on doing their job at hand, whether that is designing a building or playing a game. Security procedures would be a distraction and an overhead that would diminish their primary activity (see Table 1 above). Security is the job of professionals, if done well. As Angela Sasse (2014) put it:

‘The role of security is to be a long-term business enabler. Security measures must not get in the way, and the time and effort security consume must be well contained (Herley forthcoming). Security must require less time and effort, not more. Security should be mostly done by security professionals - yes every individual has to take some responsibility, but the time and effort associated with it has to be contained to a point where individuals can still lead productive lives. Currently, security professionals are doing a lousy job, where they stick on all sorts of countermeasures that aren't very effective, but they require lots of detailed knowledge and effort. They are the ones who have to clean up their act, so the rest of the world can get on with their lives and stay secure by sticking to a simple set of rules.’

So, least one think that a security mindset is a common sense approach, it might well run counter to mainstream views on the need for security professional to do better jobs so that users can put security in the background, to put it out of their minds, so they can focus on the instrumental purposes of their online activity. However, a security mindset might be more or less out of mind in that it is not creating a constant overhead for users, but is conditioning their work. They do things to protect their security without thinking about it. This is the way one works – it is a routinized process innovation.

Another, somewhat similar albeit different approach has also placed more of a focus on users and what might be called ‘attitude change’. In this case, research has dealt with beliefs, attitudes and values, as well as practices around cybersecurity. For instance, my own work on Internet
users has examined attitudes, values, beliefs and practices of relevance to security (Dutta 2010; Dutton 2014). Do users of the Internet value security, believe it is an important criterion, and do things to protect their security? How do they weigh security relative to other, possibly competing values, such as freedom of expression? What this research does indicate is wide variation in perceptions of risk, and the adoption of practices widely viewed as mindful of security. In short, it is arguable, based on current research that a cyber security mindset does not exist.

There could be a shift of perspective in research but also in policy if focused on a security mindset. It could imply that attitudes about security are not continually balanced with other values and attitudes in making decisions, but that security provides a context or framework from which other choices are made. A user simply does not make choices that are independent of their perceived implications for security. The need for security is taken for granted, and decisions that undermine security become risky if not untenable.

Empirically, this may mean that we would not only expect more uniformly positive attitudes toward cybersecurity, if such a mindset exists, but also that a set of attitudes and values toward cybersecurity shape other attitudes, values, and choices. There would be a causal link, not simply a different mix of attitudes.

In addition, as a mindset, the need for security would be unquestioned or not continually revisited. It would be viewed not as an optional burden, but as a cost of doing business. A reasonable level of security would be viewed as a necessary albeit not sufficient condition for the use of the Internet. It would not be an ad hoc criterion of choice, but a routine and learned as an almost instinctual response set.

What difference would such a framework make for policy or practice? First, it could be functional to introduce the concept as an aim of cybersecurity initiatives. Other issues of Internet policy have been usefully introduced as aims, such as those of closing the digital divide, or addressing the skills gap across users. The very idea of a cybersecurity mindset could foster an alternative to security as a burden or imposition that creates problems for users. Discussion following from this
idea could also contribute to fostering a security mindset from the bottom-up. As Cook (2014) argued:

“One thing that would help is a method and an agreed language that can enable the qualitative assessment of these security risks and the mindset to approach security in a risk-managed manner. This could help government shift from lagging in many areas of 'cyber security' to leading a (global) adoption of a more risk managed approach to security that is chosen and owned by all the parties responsible for the systems and services, using a consistent approach. This may also help in the currently complicated area of (Internet) governance, public perception of government influence and the politics of large scale public procurements, ....”

The idea also suggests what not to do. It is likely to be a bad idea to impose security from above, as a matter of policy rather than a matter of social choice. Also it will be important to juxtapose and contrast a security mindset with less functional perspectives, such as an unwarranted culture of fear, or alarmist rhetoric. The explication and elaboration of a healthy cybersecurity mindset could be the first step in fostering a new approach to cybersecurity that diffuses among users, much like bike security.

More specifically, the idea of a security mindset reinforces the need to broaden notions of cybersecurity. It is no longer simply in the purview of computer science departments, and technical experts. Notions of cybersecurity need to be more widely cast, as Cook (2014) explains:

“Of course, one of the principal downsides of qualitative risk assessments is a reliance on 'experts' and the quality of the experts can be hard to determine or measure (it can also be easy to expect too much of them). However, I think it is possible to source, educate and train people to the point that we have a critical mass that are 'independent' of commercial interests and 'government' and can make assessments and suggest appropriate measures to manage the risk.”

However, might there be risks of promoting a cybersecurity mindset, such as in undermining other key values of a safe and open Internet, such as freedom of expression and privacy? This
must be a key question. In theory, a security mindset could actually protect freedom of expression; just as traffic laws enable individuals to go anywhere they wish to go as long as they drive safely. But in practice, is there a risk of greater acceptance of security concerns having a chilling effect on freedom of expression, such as by legitimizing greater security. Likewise, might privacy be undermined by a greater priority being placed on security? Perhaps it will be part and parcel of the security mindset that cybersecurity is a means to ensure freedom of expression, privacy and other key values of an open Internet.

The cybersecurity community should consider whether it should move forward with the idea of a cyber security mindset as one means of ensuring a broad participation that moves beyond the experts, and security specialists, to incorporate users and practitioners at all levels. Should a security mindset be viewed as a goal, or should security be out of the mind of users and in the hands of more capable security professionals? Do we need a security mindset, or simply more supportive attitudes toward cyber security on the part of users? Hopefully this brief note will help foster the discussion needed to refine these ideas, bring them to a wider community, and lead to further research on the logic, practice and implications of fostering a cybersecurity mindset.
References


