INTERNET POLICY REVIEW
Journal on internet regulation

Volume 6 | Issue 1

Fostering a cyber security mindset

William H. Dutton
Quello Center, Michigan State University, East Lansing, United States, wdutton@msu.edu

Published on 19 Jan 2017 | DOI: 10.14763/2017.1.443

Abstract: Cyber security experts have acknowledged the need to focus more attention on the attitudes, beliefs and practices of end-users. Unfortunately, rather than fostering social research on users, this realisation has more often led to blaming users for security problems and sponsorship of fear-based campaigns directed at end-users. This scholarly essay argues for a shift in research to center on fostering a 'security mindset'. Instead of just identifying safe practices, this would help build a mindset that embeds cyber security considerations into the everyday choices of users. This paper seeks to explain the concept of a security 'mindset' and its social significance, and suggest ways to move research forward.

Keywords: Cyber security, Cybersecurity, Security, Mindset, User behaviour

Article information

Received: 27 Sep 2016 **Reviewed:** 07 Dec 2016 **Published:** 19 Jan 2017

Funding: This article was supported in part by the Oxford Martin Global Cyber Security Capacity Centre at the University of Oxford, and in part by the Quello Center at Michigan State University.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/fostering-cyber-security-mindset

Citation: Dutton, W. H. (2017). Fostering a cyber security mindset. *Internet Policy Review*, *6*(1). https://doi.org/10.14763/2017.1.443

This essay is an updated revision of a working paper for the Capacity Center (Dutton, 2014).

Acknowledgments: The author would like to thank Kristofer Erickson, Sean Lawson and Nathalie Maréchal for their insightful comments on this version as well as Ruth Shillair, Barbara Ball, and the editor for valuable comments on an earlier draft.

INTRODUCTION

Cyber security is a broad concept, which encompasses the "technologies, processes, and policies that help to prevent and/or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technology by a hostile or malevolent actor" (Clark et al., 2014: 2). It involves physical security as well as cyber security, such as protection from insider threats. It entails all levels of the internet and all the many actors

involved in the provision and use of the network, from those governing and building this infrastructure to the diverse array of end-users.

Given this broad definition, who then is responsible for cyber security? While responsibility is most often contingent on the specific activity and context, it is increasingly clear that the worldwide diffusion of the internet and its appropriation into everyday life has dissipated this responsibility far more than in early stages of computer-mediated media, information and communication systems to involve a wide array of actors across multiple layers of the internet - from internet use to its global governance (DeNardis, 2014; Schneier, 2015).

More specifically, the worldwide adoption of the internet has enabled end-users not only to access information from around the world, but also to create and otherwise source their own information for the world. In many respects, this has empowered users, as is illustrated by the many ways users are able to challenge those in positions of influence, such as the press, with countervailing information (Dutton, 2009; Dutta et al., 2011). However, it has also meant that responsibility for the security of information resources on the internet has devolved to include users around the world and the institutions in which they are involved and not only the technical experts engaged in cyber security.

This does not mean that end-users should be expected to be responsible for their own security online, but they are expected increasingly to have some shared responsibility with other actors. Creating systems that would centrally protect end-users would also undermine their role in creating and using the internet in powerful ways. Put another way, the protection of cyber security is no longer lodged solely with the computer experts in some centralised department of information technology within a user's place of work or with their internet service provider. It is distributed globally across over 3.6 billion internet users who share some responsibility in this process with a multitude of other actors.

Unfortunately, this realisation has not been accompanied by strong programmes of research aimed at understanding the attitudes, values, and behaviour of users with respect to cyber security. There have been a growing number of initiatives seeking to bring the social sciences into work on cyber security, such as by the University of Maryland's Cybersecurity Center (MC2), the University of Sydney's Cyber Security Network, the iSafety Lab at Michigan State University, and the Oxford Martin Global Cybersecurity Capacity Centre at the University of Oxford, which defines social and cultural factors as key dimensions relevant to developing a cyber security capacity (Whitty et al., 2015). Also there have been many studies focused on particular communities of users exposed to security risks, such as for digital rights activists, bloggers, whistleblowers and journalists (e.g., Coleman, 2014), the victims of romance scams (Whitty & Buchanan, 2012), or consumers involved in online banking (Shillair et al., 2015). In the neighbouring area of privacy research, there has been much work done over decades on the beliefs, attitudes and values of computer and internet users, including motivations behind their actions relevant to protecting personal information from unauthorised disclosure (Acquisti and Grossklags, 2008; Bennett and Parsons, 2013). But arguably, a focus on technical issues of cyber security, such as standards, has overshadowed work on the social and cultural issues.

Moreover, with some exceptions, most social and cultural research initiatives have focused on the development of awareness campaigns, information campaigns designed to alert users to security risks. Awareness campaigns have been prominent in a wide range of areas, particularly in research on health behaviour, where social psychologists and other social scientists have sought to convey threats and also change behaviour in ways that might mitigate risks in such areas as anti-smoking and safe sex campaigns. However, translating awareness into behavioural

change has been the central difficulty in all strategies, even with smoking and safe sex, where the behavioural response is relatively simple to convey (Rice & Atkin, 2013). In cyber security, the risks are more difficult to communicate, given the multiplicity of risks in particular circumstances, and the remedies, which are often difficult for end-users to implement. Too often, the design of systems make more secure practices less usable (Nurse et al., 2011).

In the cyber security area, awareness campaigns are essentially focused on generating fear among users, fear that they will be harmed if they do not follow safe practices (Bada and Sasse, 2014). Yet seldom are these fear campaigns accompanied by clear instructions on best practice nor are they useable and acceptable, such as memorising dozens of more complex passwords and frequently changing them (Whitty et al., 2015). For example, regularly updating anti-virus software is a common recommendation, but many users have expired or outdated anti-virus software (Batchelder et al., 2014). There are even videos online about how to turn off anti-virus software as it is often required to install new software. Simplistic practices in the eyes of security practitioners often fail as useful guides to end-users. Fear campaigns can have a chilling effect and otherwise be counterproductive if they are not tied to clear approaches to addressing the problem (Lawson, 2016).

It is arguable that fear campaigns might work in some areas, such as health campaigns on smoking, where there is a clear response (stop smoking). But failure is common even in these areas, since behavioural change is dependent on messages being well produced and anchored in strong social psychological theories of behaviour change (e.g., Bandura, 1991; Rice and Atkin, 2013). In the area of cyber security, they have proven less effective, as the threats and solutions are ever changing and the problems seem to be mounting (Bada and Sasse, 2014; Bauer and Dutton, 2015; Shillair et al., 2015). Rather than simply blame users for not following safe cyber security practices, more focus needs to be placed on designing systems for which security practices are more useable, such as reflected in moves toward the use of more biometric data. However, this is particularly difficult given the diversity of uses and contexts of use around the internet. It was in the context of these dilemmas that I stumbled upon the concept of a cyber security mindset.

THE IDEA OF A CYBER SECURITY MINDSET

In a conversation at a workshop on cyber security, Alastair Cook (2014), Director of Critical Insight Security Ltd., argued that the challenges in this area required a security mindset among internet users, which I would define as a set of attitudes, beliefs and values that motivate individuals to continually act in ways to secure themselves and their network of users, such as by acquiring technical skills, new practices or changing their behaviour online. This is not necessarily the adoption of a particular set of practices or habits, like changing your password, since secure behaviour will change over time and across contexts. It could however involve keeping an open mind to changing cyber security threats and practices.

The idea is that users need to prioritise cyber security in all aspects of their online behaviour as a matter of course. Rather than following a learned set of practices or habits, individuals could internalise this goal in ways that it motivates them to prioritise security in their online behaviour. As noted above, research has begun to explore attitudes toward cyber security, as well as the practices of users with respect to security. However, could the concept of a 'security mindset' be a subtle but important shift away from more common notions of the priority given to security attitudes and practices, such as habits?

Is this indeed a significant shift in thinking about cyber security? Can the concept of a security mindset be conceptually defined and empirically operationalised? Perhaps it is also a more qualitative shift to a sensitising 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?

REASONING THROUGH ANALOGY – WITH A BICYCLE

An analogy might be useful before I try to develop the concept more precisely. Any analogy is inherently inaccurate of what it represents, and better analogies might be suggested, but the example of bike security came immediately to mind when faced with the idea of a cyber security mindset.

Since I had lived in Oxford for over a decade, where bikes are a major mode of transportation, and routinely biked to work, it was clear that nearly all bike riders in this city had a security mindset. For instance, 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 are not going through a threat assessment each time they purchase a bike or get on their bike. 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. In such ways, bike riders in Oxford feel as if they know what to do in order to better secure their bikes. They have a sense of personal efficacy associated with bike security.

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 socially supported 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.

In contrast, bike safety – not security – might be less of a mindset in that you can see wide variation among bike riders. Some equip themselves with helmets, reflective clothing, and more, while others do not. Riders are more likely to go through a process of threat modeling, such as weighing the choices on whether or not to use a helmet, depending on where they are riding and what they are wearing, than on whether to secure their bike. Should I stay behind the bus, and have a 100% chance of losing my momentum, or veer around the bus with a 1% chance of being hit by a car? Safety might be a mindset for some, but it appears less universal and more flexible than a bike security mindset.

A BIKE IS NOT A COMPUTER NETWORK

Of course, protecting a bicycle is very different from protecting a computer device, or personal information in the cloud. I would argue that this makes the analogy all the more powerful, since

it moves discussion away from specific practices or rules that vary across different technical systems. Instead, it highlights the personal and social factors behind a motivation for security practices, whatever they may be.

That said, some have raised problems with my bike analogy. The first concerns the visibility of the security issue. You know sooner or later when your bike has been damaged or stolen, but it is often far more difficult to detect whether your networked computing resources have been tampered with, copied, or disclosed without your authorisation. Increasingly, breaches of a computer can leave no physical evidence of being compromised, such as not changing its performance. Perhaps this difference in transparency or visibility suggests a direction for supporting a cyber security mindset. The visibility of spam, for example, enabled spam filters to be widely accepted and used. The visibility of a stolen bike or a breach of your computer could help foster a security mindset.

Another concern raised was over the degree that individuals who have poor security practices in relation to computer networks are likely to have consequences for those with whom they communicate, while the consequences of a stolen bike are likely to rest more squarely with the individual who failed to secure it. In this case, I find the bike analogy valuable, despite this difference, because there is clear social pressure to adopt a bike security mindset even when the consequences are less networked. Again, the visibility of not following these practices could be a key difference. When friends realise a problem with another person's bike or computer security, such as when they receive spam from a friend, they do sanction their friends. Visibility or transparency might be key to building a cyber security mindset by also enhancing the likelihood of peer social influence.

DEFINING A MINDSET

The idea of a 'cybersecurity mindset' arose from qualitative interviews, conversations with cyber security researchers and practitioners, and participant-observation around the social aspects of cyber security. Within a qualitative tradition, this concept, like many other qualitative concepts is what Herbert Blumer (1954) has called a "sensitizing concept". That is, the concept helps to sensitise the reader to a complex set or patterns of concrete empirical observations. It is not a quantitative concept that is operationally defined, such as by answers to questions or by specific behaviour. It is more flexible, and does not have a definitive set of empirical attributes since it could be manifested in different ways across time or contexts. It is in this tradition that I am employing the concept of cyber security mindset, as a 'sensitizing concept' within a qualitative perspective of social research.

So – what is in a mindset? As noted above, I have defined a cyber security mindset as a pattern of attitudes, beliefs and values that motivate individuals to continually act in ways to secure themselves and their network of users. 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. In other contexts, a mindset has been usefully defined as 'how we receive information' (Naisbitt, 2006: xvii). For example, the same information, such as an email attachment, will be received in different ways if one has a cyber security mindset. And 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 the social influence of friends and fellow users, and sources of information chosen by users.

Different actors, such as cyber security experts versus end-users, will manifest a cyber security mindset in very different ways. For example, the security experts with such a mindset would be constantly considering ways that a technical system could be breached as these mental scenarios will lead them to design systems and train users to avoid the problems they anticipate. Users are unlikely to think about how malicious users might try to steal their information, but they are likely to consider ways to keep the protection of their equipment and network resources safe from others, if they have a cyber security mindset.

It is immediately apparent that a mindset is not a dichotomous state. It is not that you have it or you don't. For example, a security mindset might be exaggerated in ways, such as being so disproportionate to the risks, that it 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 when many universities and colleges postponed the adoption of wireless internet access because it was viewed as insecure. Their security mindset was focused on protecting the institution, but not balanced with the interests of the end-users. The flip side of this is the reputed disregard for 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, or changing the default password on the wireless router.

These two extreme examples suggest that a security mindset can err on either being set too high or low, exaggerating or underestimating 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 (Gerbner and Gross, 1972; Glassner, 1999). More generally, moral panics over the use of social media have become a serious issue (Krotoski, 2014). Therefore, in fostering a security mindset, it is critical as well not to foster a culture of fear. In fact, many banks and other business enterprises worry about communicating security breaches least they have a chilling effect on the use of online systems by their customers (Bauer and Dutton, 2015). In the area of copyright and the 'theft' of software or content, fear campaigns have been so dramatic and exaggerated that they have been lampooned by critics (David, 2013). In this respect, a security mindset is a potentially valuable alternative to creating a culture of fear. In the bike analogy, there is also no guaranteed security with a lock that can be cut, but it would be a disproportionate response for people to stop riding their bikes least they inevitably must leave them in public places.

The bike example also suggests that the high cyber security 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, as suggested above, it could be up to them to protect the institution. In this sense, adoption of a security mindset would be in the interest of all actors in the larger context of users.

More importantly, however, it is unclear that the experts in IT can continue to protect institutions and the public on their own, given the nature of the internet and web and social media, which will be exacerbated by the rise of the Internet of Things (IoT). As Alastair Cook (2014) put it:

> If you ask an IT security person 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 need to be enrolled in 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). Over time, as current security practices become outdated, such as reliance on passwords, technical knowhow might well diminish in importance, relative to the motivations of users that are anchored in more social and psychological processes.

DIRECTIONS FOR RESEARCH

Social science research on cyber security is relatively new when compared to social research on many other issues tied to computing and the internet, such as privacy, which has been central to social research since the earliest days of the domestic use of computers (Bennett and Parsons, 2013). The movement of more social scientists into the study of cyber security is a major new direction for the research in this area. This more multidisciplinary turn in cyber security research should be recognised and supported.

In cyber security research, there has been much attention to the formation of good practices and habits that promote safety online (e.g., Anderson and Agarwal, 2010; Johnston and Warkentin, 2010; Boss et al., 2015). For example, there is a stream of research that seeks to examine protection motivation theory (PMT) in the context of safe computing (e.g., Shillair et al., 2015; Vance et al., 2012). PMT theory has been anchored primarily in research on pro-health messaging, such as around anti-smoking and safe sex campaigns. It has identified a set of factors that lead to safer behaviours and the formation of good habits. These include the feeling that the potential threats are serious, and that the person believes they have a reasonable likelihood of being vulnerable. This forms a basis for many fear-centric campaigns. But PMT also posits that personal efficacy in dealing with the threat, and the efficacy of a recommended action, such as to stop smoking or practice safe sex, are critical to developing good practices. Getting into the habit of not smoking is a strong recommendation that people know how to do, even if they often have difficulty doing so.

Cyber security is different. The threats often seem more remote and less likely, hence a focus on fear campaigns to compel a sense of immediacy of threat. However, internet users develop a learned level of trust in the internet through their experience online, as the internet is an ‘experience technology’ (Dutton and Shepherd, 2006). If they are unaware of their computers or smartphones being compromised, and their experiences are overall positive, their trust in using the internet can grow, despite real threats.

Also, there is a greater problem with many internet users feeling like they know what to do, and have the background and wherewithal to do it, but they put it off in lieu of convenience or useability, such as memorising many passwords and frequently changing them. Moreover, if internet users get into poor habits, such as using the same passwords, then they are more subject to cyber security threats. In many respects, they need to habitually avoid routine habits that might increase their vulnerability. These differences may make cyber security different from other areas of research on PMT, making it somewhat less applicable. A cyber security mindset might well be one in which internet users are aware of the need to not just rely on old habits but rather to continually be aware of new threats and new protective measures.

Another stream of research is focused on mental models of users, such as how they think cyber

security works (Wash and Rader, 2011). Poor mental models of how the internet works or how cyber security can be threatened could be a major aspect missing from the knowledge that is essential to protecting one's security. Lacking such knowledge could be one element undermining the personal efficacy of internet users, and therefore their propensity to protect themselves. However, in many areas, from producing television to computing, efforts to explain how these systems work tend to leave their audience more mystified, rather than more well informed. But a cyber security mindset is not equivalent to a mental model of cyber security. It is an almost unconscious propensity to act in ways that help keep a user more secure. They do not have to think through all the aspects of how the internet works. Gaining the knowledge and skills to achieve this state of mind is of course a likely route to explore.

Other work by Whitty and others (2015) have looked at the social and psychological factors shaping the use of passwords. My own work on internet users has examined attitudes, values, beliefs and practices of relevance to security (Dutta, 2010; Dutton et al., 2014). Do users of the internet value security, believe it is an important criteria, and do things to protect their security? How do they weigh security relative to other, possibly competing values, such as freedom of expression? This research indicates wide variation in perceptions of risk, and the adoption of practices widely viewed as mindful of security. From this limited research, it is arguable, based on current research, that most end-users lack a cyber security mindset.

However, previous research on the social aspects of cyber security has not focused on the notion of a mindset, but has dealt with beliefs, attitudes and values, as well as practices around cyber security habits. 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 simply balanced with other values and attitudes in making decisions, but that security provides a context or framework from which other choices are made. In this new perspective, 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. While this is the ultimate objective, the reality at present is that users normally make choices independent of security. They make choices based on other objectives, such as usability or convenience, but seldom on the basis of security (Furnell, 2008).

Empirically, this may mean that we would not only expect more uniformly positive attitudes toward cyber security, if such a mindset exists, but also that a set of attitudes and values toward cyber security shape other attitudes, values, and choices about the internet and online services. There might well be a causal link between the existence of such a mindset and safer behaviour, such as reflected in fewer bad experiences with security.

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. And, as in the case of bike security, an end-user's behaviour would be more significantly influenced by social influence and modeling of the behaviour of those who have such a mindset, than by top-down efforts to instilling fear on the part of the user.

IMPLICATIONS FOR RESEARCH

The argument of this essay has been on the need for considering the potential of shifting social science research on cyber security to include a focus on the concept of a cyber security mindset and various social scientific perspectives that could inform its role in shaping behaviour. However, there is a prior need for more social research to assess the value of such a focus. For example, it is unclear exactly whether a cyber security mindset could be operationally defined. To approach this issue, research needs to first identify individuals that on the basis of qualitative observations appear to have a cyber security mindset. For example, qualitative or quantitative research on end-users might be used to locate individual internet users who perceive themselves to be highly effective in coping with cyber security threats. Then we would need to study what they do, as well as what they say they do.

Work in line with this idea is underway in research that Sarah Myers West and her colleagues at the Annenberg School at USC are pursuing on the practices of digital rights activists, who are very aware of the potential for their online activities to be monitored. I am working with Ruth Shillair on how sophisticated internet users can more effectively engage in the cat and mouse game with malicious users, such as by choosing where they go for information about risks and how to respond (Shillair and Dutton, 2016).

Just as some of the best studies of science are focused on normative and descriptive research on how scientists do what they do (Latour and Woolgar, 1979; Diesing, 1992), there could be much value to studying those internet users who appear to have a strong cyber security mindset. Once we know more about their attitudes and practices, we can then identify others with this mindset, and also discern the contexts and demographic factors shaping the acquisition of this mindset, as well as what difference it makes. Do people with a cyber security mindset fare better against the shifting threats to their security online?

IMPLICATIONS FOR POLICY AND PRACTICE

What difference would such a framework make for policy or practice? First, it could be helpful to introduce the concept as an aim of cyber security 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 cyber security 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. 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 "cybersecurity" 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. Mandating how people should think about cyber security is inherently problematic. Also it will be important to juxtapose and contrast a security mindset with less useful perspectives, such as an unwarranted culture of fear, or alarmist rhetoric. The explication and elaboration of a healthy cyber security mindset could be the first step in fostering a new approach to cyber security.

More specifically, the idea of a security mindset reinforces the need to broaden notions of cyber security. It is no longer simply in the purview of computer science departments, and technical experts in security, but more multidisciplinary. Notions of cyber security 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 is (sic) "independent" of commercial interests and "government" and can make assessments and suggest appropriate measures to manage the risk.

There is a need for research on a cyber security mindset to reach an increasingly diverse and global ecology of cyber security researchers. This is one means to broaden conceptions of the actors involved in cyber security beyond the experts and security specialists, and to incorporate users and practitioners at all levels. While the strategies and tactics will vary widely over time, and across the multitude of actors involved at each layer of the internet, they all could benefit from holding a cyber security mindset. Hopefully this article will help foster the discussion needed to refine these ideas, and bring them to a wider community.

CONCLUSION: A PATH TO PRETTY GOOD CYBER SECURITY

One of the early innovations in software to support the privacy of personal communication was open source data encryption and decryption software that its inventor, Philip Zimmermann, called "pretty good privacy", and which led to the foundation of a company by that name – PGP and the wide use of OpenPGP and GNU Privacy Guard (GPG). Zimmermann argued that PGP encryption would not solve all privacy problems for computer users, but that it was pretty good and would go far towards reducing invasions of personal communications.

Similarly, there is unlikely to be any absolute solution to cyber security. There is no silver bullet to stop threats to security, either through some type of technological measure or new user practice. Instead, grappling with cyber security will be a continuing process, what many have called a "cat and mouse game" between the good and bad actors, those addressing cyber security threats, and those developing malware and carrying out malicious attacks (ENISA, 2016). However, given the widespread and growing responsibility for cyber security on the part of internet users, it is essential that policy and practice aim toward the development of the beliefs, attitudes and values that lead users to continually work towards securing themselves and their network of users, such as through acquiring technical skills, or new practices and routines.

The rise of a dialogue about a cyber security mindset might help the world move in this direction. It would move the focus away from generating fear campaigns, and towards the development of ways in which internet users feel effective in securing pretty good security in their everyday lives. This is not an argument of instilling a short list of practices that users should habitually follow. Some habitual practices can create a target for malicious actors, such as using a particular form of password. If everyone had a cyber security mindset, the internet would be a safer place to obtain information and communicate with others. And by trusting more in the bottom-up processes of user innovation and social pressure in response to security threats, internet users are more likely to challenge malicious actors and also state actors engaging in well-intentioned but unwarranted surveillance.

However, to progress towards this future, research will need to move away from models based on pro-health and other awareness campaigns that have more obvious sets of safe practices. We need research anchored in cyber security challenges and behaviour, as well as other related online issues, such as over user perspectives on privacy and surveillance. There is a need to identify those with a cyber security mindset, understand how to diffuse this mindset, and what impact its acquisition is likely to have on cyber security. At the same time, it is important to recognise that a cyber security mindset is but one possible aspect of social and cultural dimensions of cyber security that need to be addressed alongside allied efforts to enhance educational, technical, organisational, business, policy, and regulatory approaches to cyber security.

REFERENCES

Acquisti, A., & Grossklags, J. (2008). What can behavioral economics teach us about privacy? In Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & De Capitani di Vimercati, S. (Eds.), *Digital privacy: Theory, technologies, and practices* (pp. 363-380). Boca Raton, FL: Auerbach Publishers.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613–643. doi:10.2307/25750694

Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK. Retrieved from http://discovery.ucl.ac.uk/1468954/.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational behavior and human decision processes*, *50*(2), 248–287. doi:10.1016/0749-5978(91)90022-l

Batchelder, D., Blackbird, J., Henry, P., Iyer, S., Jones, J., Kulkarni, A., … Zink, T. (2014). *Microsoft Security Intelligence Report | January through June, 2014* (Microsoft Security Intelligence Report No. 17). Microsoft Corporation. Retrieved from https://www.microsoft.com/en-us/security/operations/security-intelligence-report

Bauer, J. M., & Dutton, W. H. (2015). *The new cybersecurity agenda: Economic and social challenges to a secure internet* [Working Paper]. Oxford Global Cybersecurity Project at the Oxford Martin Institute, University of Oxford, and the Quello Center at MSU. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2614545/.

Bennett, C. J., & Parsons, C. (2013), Privacy and surveillance: The multidisciplinary literature on the capture, use, and disclosure of personal information in cyberspace. In Dutton, W. H. (ed.), *The Oxford handbook of internet studies* (pp. 486-508). Oxford: Oxford University Press.

Blumer H. (1954), What is wrong with social theory? *American Sociological Review*, *19*(1), 3–10.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What Do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. *MIS Quarterly*, *39*(4), 837–864. doi:10.25300/misq/2015/39.4.5 Retrieved from http://papers.ssrn.com/abstract=2607190/

Clark, D., Berson, T., & Lin, H. S. (Eds.) (2014). *At the nexus of cybersecurity and public policy*. Washington, DC: The National Academies Press.

Coleman, G. (2014), *Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous*. London: Verso.

Cook, A. (2014). Personal communication via email, 23 June 2014. Alastair Cook permitted me to paraphrase his comments at a workshop on 19 June 2014.

David, M. (2013). Cultural, legal, technical, and economic perspectives on copyright online. In Dutton, W. H. (Ed.), *The Oxford handbook of internet studies* (pp. 464–485) . Oxford: Oxford University Press. doi:10.1093/oxfordhb/9780199589074.013.0022

DeNardis, L. (2014), *The global war for internet governance*. New Haven, CN: Yale University Press.

Diesing, P. (1992). *How does science work? Reflections on practice*. Pittsburg, PN: University of Pittsburgh Press.

Dutta, S., Dutton, W. H., & Law, G. (2011). *The new internet world: A global perspective on freedom of expression, privacy, trust and security online: The Global Information Technology Report 2010–2011*. New York: World Economic Forum, April. Retrieved from SSRN: http://ssrn.com/abstract=1810005/.

Dutton, W. H. (2009), The fifth estate emerging through the network of networks. *Prometheus*, *27*(1), 1–15. doi:10.1080/08109020802657453

Dutton, W. H. (2014). Fostering a cybersecurity mindset. A draft working paper. Oxford, UK: Global Cyber Security Capacity Centre. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CybersecurityMindsetDraftWorkingPaper.pdf/

Dutton, W. H., Law, G., Bolsover, G., & Dutta, S. (2014). *The internet trust bubble: Global values, beliefs and practices*. New York: World Economic Forum. Retrieved from http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf/.

Dutton, W. H., & Shepherd, A. (2006). Trust in the internet as an experience technology. *Information, Communication and Society*, *9*(4), 433–451.

ENISA (2016, January). European Union Agency for Network and Information Security, *ENISA threat landscape 2015*. Brussels: ENISA.

Furnell, S. (2008). End-user security culture: A lesson that will never be learnt? *Computer Fraud and Security*, *2008*(4), 6–9. doi:10.1016/S1361-3723(08)70064-2

Gerbner, G., & Gross, L. (1972). Living with television: The violence profile. *Journal of Communication 26*(2), 173–199.

Glassner, B. (1999). The culture of fear: Why Americans are afraid of the wrong things. New York, NY: Basic Books.

Johnston, B. A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549–566. doi:10.2307/25750691

Krotoski, A. (2014). Inventing the internet: Scapegoat, Sin eater, and Trickster. In M. Graham, & W. H. Dutton (Eds.), *Society and the Internet* (pp. 23–35). Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780199661992.003.0002

Latour, B., & Woolgar, S. (1979, 1986), *Laboratory life: The construction of scientific facts*. Guildford, Surrey: Princeton University Press.

Lawson, S. T., et al. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. *In Cyber Conflict (CyCon), 2016 8th International Conference on* (pp. 65–80). IEEE.

Naisbitt, J. (2006), *Mindset!* New York: Harper Collins. doi:10.1109/cycon.2016.7529427

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. 2011 Third International Workshop on Cyberspace Safety and Security (CSS), 21–26. doi:10.1109/CSS.2011.6058566

Rice, R. E., and Atkin, C. K. (2013) (Eds.), *Public communication campaigns*, 4th edition. Los Angeles, CA: Sage.

Schneier, B. (2015), *Data and Goliath: The hidden battles to collect your data and control your world*. London: W. W. Norton & Company.

Shillair, R., & Dutton, W. H. (2016), Instilling a cybersecurity mindset: Getting users into the cat and mouse game. Arlington, VA: TPRC, George Mason University.

Shillair, R., Cotten, S. R., Tsai, H. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me□: Convincing internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. doi:10.1016/j.chb.2015.01.046

Vance, A., Siponen, M., & Pahnila, S. (2012), Motivating IS security compliance: Insights from habit and protection motivation theory, *Information and Management*, *49*(3-4), 190–198. doi:10.1016/j.im.2012.04.002

Wash, R., & Rader, E. (Eds.) (2011). Influencing mental models of security. Proceedings of the New Security Paradigms Workshop (NSPW): Marshall, CA. September.

Whitty, M. T., & Buchanan, T. (2012). The online dating romance scam: a serious crime. *CyberPsychology, Behavior, and Social Networking*, *15*(3), 181–183. doi:10.1089/cyber.2011.0352

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015), Individual differences in cyber security behaviours: An examination of who's sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. doi:10.1089/cyber.2014.0179