Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape

Vladlena Benson[a], John McAlaney[b] and Lara Baranowski[c]

a. Chair in Cyber Security, University of West London, London, UK; email: vladlena.benson@uwl.ac.uk

b. Senior Lecturer, Department of Science and Psychology, Bournemouth University, Bournemouth, UK

c. Senior Lecturer, Criminal Psychology, Open University, London, UK.

Human Element: Cyber Security Starts Here.

Cybersecurity professionals agree that that security depends on people more than on technical controls and countermeasures. Recent reviews of the cyber security threat landscape show that no industry segment is immune to cyber-attacks and the public sector tops the list for targeted security incidents (Benson, 2017). This is largely attributed to the weaker cyber security mindset of employees. On the other hand, the financial sector year on year experiences the highest volume of cyber breaches aimed at financial gain or espionage. What is common between these rather different sectors is that the attack vector by cyber criminals starts with social engineering the weakest link in their security chain. With the continuous loss of control over personal information exposed online (Benson et al., 2015) individuals present easy targets for non-technical attacks ranging from spear-fishing to whaling leading on to serious cyber victimisation.

Though human behaviour in online contexts has been addressed by researchers for some time, the cybersecurity industry, policymakers, law enforcement, public and private sector organizations are yet to realise the impact individual cyber behaviour has on security. It is important that this gap is addressed. A secure system is one which behaves in a predictable and rationale way; however as demonstrated by psychological research human behaviour and decision-making processes are multifaceted and often unpredictable. In order to improve cybersecurity practices there is a need for discussion that acknowledges that cybersecurity is inherently a complex socio-technical system. This concept is not new in psychological research. Indeed in 1951 Trist and Bamforth proposed the idea that changes to a technological system must be complemented by changes to social systems. To do one without the other could result in a systems failure. If one is concerned about cyber security, the human element must be investigated in depth. If the human element is not considered where human behaviour is involved, the system is doomed to failure before it begins.

To gain better insights in addressing evolving challenges of the digital world, Cybersecurity increasingly relies on advances in human behaviour research. Whilst technology may often form the core of cyber-attacks, these incidents are instigated and responded to by humans. As demonstrated in recent cybersecurity breaches, such as the WannaCry ransomware affecting 150 countries, cybersecurity incidents exploit the human element. Cyber threats are

increasingly choosing psychological manipulation, known as social engineering, rather than hacking in the traditional technical sense. To effectively integrate technology with the human element, a number of fields can be looked to for guidance. The military and intelligence community have been dealing with this for some time; banking and financial industries as well. Both use aspects of psychology and the human element to better detect fissures in security. If we were to ignore basic psychological research would be doing a disservice to the cybersecurity field. Understanding decision making, vigilance, and sheer convenience which undoubtedly play a role in security are essential features to understanding how to keep ourselves safe in an increasingly cyber world. Making sure that the way that employees think about keeping company data secure should match habit and personality style. Requiring frequent password changes may not be an effective strategy as people are less likely to do that then come up with a single intricate password that they use for a year. Thinking about matching the behaviours with the person is an effective strategy, we look into aligning theory to existing experiences in order to answer the following questions:

1) Can psychological manipulation of a cyber victim be countered by technical controls? – current threats mitigation measures try to establish 'expected' user profiles and identify unusual behaviours.
2) Can lapses in decision making have a measured impact on organisational and individual vigilance? – establishing metrics around appropriate decision making can help reflect preparedness of organisations towards cyber-attacks, including those manipulating employees.
3) Will cultural differences and beliefs eventually lead to idiosyncratic cyber security mechanisms? – cyber security solutions, including authentication and detection mechanisms, follow a one-size-fit-all paradigm leading to varied effectiveness.
4) Can cybersecurity be better explained through the lens of a complex socio-technical system? – viewing a secure system as one which behaves in a predictable and rationale way creates issues when a human element is introduced into consideration.
5) What are the emerging ways to address the weaknesses of human behaviour? – achieving the secure state of mind requires more than technical countermeasures which rely not only on fear but on individual and collective human strengths.

The fight against cyber threats never stops and can be viewed as an arms race between malicious and benign actors. New areas have emerged in the field, such as the growth of commercial crimeware, the proliferation of open source hacking tools and social media enabled social engineering strategies which are worthy of attention. While for some cyber psychology is seen as a new way of doing old things, others highlight how differences in online behaviour warrant new methodological approaches to cyber security. For instance, the perceived anonymity and disinhibition effect offered by the internet is known to change human behaviour in several ways, such as altering perceptions of risk and willingness to engage in criminal behaviour.

We are in it together.

We also need to consider not just the interaction between the individual and the machine, but also how the interaction between individuals shape their cybersecurity attitudes and behaviours. Individuals do not operate in a social vacuum; the actions of the attackers and the response of the targets are in part determined by the social worlds in which they operate.

People will tend to alter their thoughts and behaviours to match the groups to which they belong (Kelman, 2006), which can include social groups, workplace group or groups of cybercriminals and hacktivists. Furthermore, emotions can spread throughout groups, even to individuals who were not involved in the incident that prompted the initial emotional response (Smith, Seger, & Mackie, 2007). In the case of hacktivism this may result in hacktivists engaging in attacks as a form of protest against targets that they have negative feelings towards, regardless of whether they have personally been affected by the actions of the target. In the case of employees within a company their response to cybersecurity threats may be influenced by the fear or stress experienced by colleagues who have fallen victim to attack such as phishing emails. In addition, the natural response of a company that has been the victim of a cyber-attack may be to hold group discussions about best to react. This is not surprising; after all humans have evolved as social creatures and we tend to draw closer together when our group is threatened. Yet it also known from psychological research that groups often make riskier decisions than an individual would alone (Wallach, Kogan, & Bem, 1962). This may apply not only to the targets of the attack but also the attackers, with both groups behaving in a riskier and possibly ultimately more damaging manner than they would have done as individuals. However, it has also been demonstrated within social psychological research that we often underestimate the extent to which we are influenced by those around us (Darley, 1992). This is an example of the type of irrationality and cognitive biases that can make the prediction of human behaviour especially challenging; not only may we misinterpret the behaviours and intentions of others we may fail to be aware of the factors that determine our own behaviour. A better understanding of how social processes influence the actions of all of the actors involved in a cybersecurity incident would improve threat prediction and help determine how to manage and optimise the response of the targets.

The importance of social norms and group identity vary between culture, ranging from those that value collectivism and acting for the good of the group to those which are individualistic and promote the success of the individual. Nevertheless, even in individualistic cultures such as the UK and USA a degree of interdependence with others is unavoidable. People working within an organisation have trust one another not to expose the organisation to cybersecurity threats through for example the opening of phishing emails. They place trust in IT services to protect them from cyber-attack, and in doing so may relegate their sense of responsibility for all computer related matters. Of course, this trust in IT services may be misplaced trust. As commented previously there is a limit to protection can be provided by technology if an individual persists in engaging in risky cyber behaviours. This relates to another well-known social psychological phenomenon known as diffusion of responsibility, in which individuals fail to take appropriate action, even in the face of impending danger, because they assume that others around them will act (Darley & Latané, 1968). These issue of trust and interdependence are not limited to the victims of cyber-attacks. Cybercrime is often a group exercise. Perpetrators rely on the skills and abilities of others to commit attacks, which requires the development and maintenance of trust. The importance of trust in such situations is arguably even more pertinent in cybercriminal gangs than in the victims they target. A betrayal by a group member may expose other group members to arrest and prosecution. The revelation that a member of the hacktivist collective Anonymous was an FBI informant could be argued to have caused more disruption within the group than did the efforts of their adversaries to dispel them. It is essential to explore these issues of group processes, trust and

social identity, and how these influence the decision-making processes of individuals and groups within socio-technical systems.

Emerging mitigation measures.

Psychologists have studied a range of topics about human behaviour and these findings must be applied to the cyber world to effectively keep people and their data secure. First, people within organisations need to be aware of the risks of cyber breaches and take them seriously. Research found that if someone has experienced a cyber threat, or has perceived such a threat, they are more likely to be vigilant (Chen & Zahedi, 2016). But, there may be ways to enhance vigilance before it comes to perceived or experienced threat. Gamification may be one way forward.

Users need to take steps to protect themselves and the data they are responsible for. Attitude may play a role. Being positive about the working environment could go a long way in increasing employee attentiveness to breaches. Trying to quell those who are disengaged with their offices or disgruntled employees who want to target the company are a worry. Corporations and employees must be vigilant and not let naivety at best and laziness or dissatisfaction with the work environment at worst come to the fore.

Behavioural nudge (Thaler & Sunstein, 2008) is another method to help ensure that company insiders are aware of the pitfalls of negligence to the very real risks of cyber breaches. Psychologists and other behaviourists have been using the concept of nudge for several years to see how it may help in altering a number of behaviours. Using these concepts for cybersecurity could be beneficial in eliciting more vigilant behaviours. Asking, and showing, employees how they could be responsible for security is essential. Changing risk taking or lackadaisical approaches could be done through nudge and yield behavioural change. If the corporations are expected to be responsible for cybersecurity and employees rely on that, there could be a breakdown in security. Creating awareness of how protection needs to be done by all users, especially in light of the incoming General Data Protection Regulations (GDPR) in May 2018, is a step in the right direction.

It will be interesting to see if the new GDPR alters the way companies deal with data protection and cybersecurity. Psychology can help with predictions as to whether the financial penalties that will be placed on companies make them more diligent. Or GDPR might encourage the company to nurture behaviour change on the part of its employees. It is believed that most people want to do the right thing so by using the regulations, nudge and by playing on aspects of personality, perhaps there will be positive changes in corporations and its employees working together to elicit secure cyber environments.

With the increasing global cyber dependency, international cyber security is not a uniform notion. In this respect aspects of psychological research show how an understanding of human behaviour can impact on keeping cyber systems secure. By considering the cultural contexts, maliciousness, personality and other such features of human behaviour, there are avenues to explore the intersection between cybersecurity and behaviour.

It is useful to review crime research as some aspects of cybercrime are similar or the same as more traditional forms of crime using new methods. Encrypting data through ransomware and requiring users to pay to have their data released is old fashioned extortion. Findings into how to deter extortion and other crimes like it may help to reduce the number of cyber

breaches. Tapping into the psychology of fear may also help the victims understand what they are experiencing and how to cope with the infringement.

Concluding remarks.

We started the discussion of key questions on psychological manipulation countermeasures and how organisational and individual vigilance can be affected by individual and collective decision making. We feel that much more research attention is necessary to help develop effective cyber security culture and address risk taking behavioural challenges.

We identified the challenges of globalisation in developing security technical solutions and opened the discussion on how culture, religion and social norms can impact controls effectiveness and taken into account when addressing the issues of cyber terrorism, propaganda and online radicalisation.

Evolving cyber threats warrant emerging ways to combat them; we see novel approaches to cyber security training, including gamification, nudging and attitude changing experiences, as the new methods facilitating collective appreciation of security objectives.

One final thought is about conducting research into cyber behaviour of individuals. As the access to data on individual digital behaviour has improved over the recent years, ethical questions became opaque. For instance, preserving anonymity of online research subjects presents issues of data 'scrubbing' and makes inferring identity straightforward. New methods are needed to ethically engage with individual users without exposing them to information breaches as shown in examples of NHS and AWS data sets exposures. As the cyber security landscape continuously changes, so are the challenges for cyber security researchers requiring agility in identifying counter mechanisms and innovation in understanding human decision-making.

References

Benson, V. (2017) *The State of Global Cyber Security: Highlights and Key Findings*. LT Inc, London, UK DOI: 10.13140/RG.2.2.22825.49761

Benson, V., Saridakis, G. and Tennakoon, H. (2015) Information disclosure of social media users: does control over personal information, user awareness and security notices matter? *Information Technology & People*, ISSN (print) 0959-3845. 28 (3), 426-441

Chen, Y. & Zahedi, F. (2016). Individual's Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China. *MIS Quarterly,* 40(1), 205-222.

Darley, J. M. (1992). Social organization for the production of evil. *Psychological Inquiry, 3*(2), 199-218. doi:10.1207/s15327965pli0302_28

Darley, J. M., & Latané, B. (1968). Bystander intervention in emergencies: diffusion of responsibility. *Journal of Personality and Social Psychology, 8*(4), 377-383.

Kelman, H. C. (2006). Interests, relationships, identities: Three central issues for individuals and groups in negotiating their social environment. *Annual Review of Psychology, 57*, 1-26. doi:DOI 10.1146/annurev.psych.57.102904.190156

Smith, E. R., Seger, C. R., & Mackie, D. A. (2007). Can emotions be truly group level? evidence regarding four conceptual criteria. *Journal of Personality and Social Psychology, 93*(3), 431-446. doi:Doi 10.1037/0022-3514.93.3.431

Thaler, R. H., and Sunstein, C.R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven: Yale University Press.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the Longwall Method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. *Human relations*, *4*(1), 3-38.

Wallach, M. A., Kogan, N., & Bem, D. J. (1962). Group influence on individual risk-taking. *Journal of Abnormal Psychology*, *65*(2), 75-&. doi:Doi 10.1037/H0044376