Incorporating Psychology into Cyber Security Education: A Pedagogical Approach

Jacqui Taylor-Jackson[1], John McAlaney[2], Jeff Foster[1], Abubakar Bello[3], Alana Maurushat[3], John Dale[4]
[1]School of Psychology, WSU, Sydney, NSW, Australia
{J.Taylor-Jackson, Jeff.Foster}@westernsydney.edu.au
[2]Department of Psychology, Faculty of Science & Technology, Bournemouth University, Poole, Dorset, UK
jmcalaney@bournemouth.ac.uk
[3]School of Social Sciences, WSU, Sydney, NSW, Australia
{A.Bello, A.Maurushat}@westernsydney.edu.au
[4]LiMETOOLS Ltd, Bournemouth, UK
john@limetools.biz

Abstract. The role of the human in cyber security is well acknowledged. Many cyber security incidents rely upon targets performing specific behavioural actions, such as opening a link within a phishing email. Cyber adversaries themselves are driven by psychological processes such as motivation, group dynamics and social identity. Furthermore, both intentional and unintentional insider threats are associated with a range of psychological factors, including cognitive load, mental wellbeing, trust and interpersonal relations. By incorporating psychology into cyber security education, practitioners will be better equipped with the skills they need to address cyber security issues. However, there are challenges in doing so. Psychology is a broad discipline, and many theories, approaches and methods may have little practical significance to cyber security. There is a need to sift through the literature to identify what can be applied to cyber security. There are also pedagogical differences in how psychology and cyber security are taught and also psychological differences in the types of student that may typically study psychology and cyber security. To engage with cyber security students, it is important that these differences are identified and positively addressed. Essential to this endeavor is the need to discuss and collaborate across the two disciplines. In this paper, we explore these issues and discuss our experiences as psychology and cyber security academics who work across disciplines to deliver psychology education to cyber security students, practitioners and commercial clients.

Jacqui Taylor-Jackson, John McAlaney, Jeff Foster, Abubakar Bello, Alana Maurushat, John Dale,
Incorporating Psychology into Cyber Security Education: A Pedagogical Approach,
Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security (FC).
February 14, 2020 Kota Kinabalu, Sabah, Malaysia Springer, 2020.

1 Introduction

Although there is a lack of empirical assessment regarding the cognitive aptitudes, communication skills and team-working needed for cyber security professions to be effective [1], in this paper we show how we have introduced psychology into cyber security programmes to ensure that professionals have an understanding of behavior to relate to their domain-specific knowledge and technical skills. Cyber security incidents are composed of a sequence of behavioural actions, each of which is determined by a range of psychological factors. In many cases cyber adversaries actively attempt to exploit and manipulate psychological processes of their targets, such as for example through the use of phishing emails. This reflects the view of humans as being the weakest link in cyber security [2]. However, despite the recognised importance of the human element it could be argued that cyber security education and training programs often neglect to fully address the psychological components of cyber security. This is despite the extensive research literature in psychology that is highly relevant to cyber security – understanding motivation, predicting future actions, designing human-centred policies and interfaces, and changing behaviour and organisational culture. These are topics that are taught within psychology programs in colleges and universities across the world, as well as within behaviour change and training courses in commerce and industry. As such there is existing experience pedagogical knowledge on how best to educate people about psychology across a range of settings, which could be better utilised for the education of cyber security students and practitioners.

This lack of interdisciplinary approaches to teaching psychology as part of cyber security could in part be explained by the nature and typical pedagogical approaches used in each discipline. Psychology is a very broad discipline; ranging from sub-topics that are highly reliant on quantitative, technological approaches such as neuropsychology, to those which are deeply rooted in qualitative approaches. There is a finite amount of time available to deliver any cybersecurity education or training; it would not be practical or desirable to deliver a course that includes all the different approaches to psychological research. In addition, some of the epistemological and ontological assumptions that are made in psychology differ from those used in cyber security and computing. As with other social science subjects many areas of psychology draw upon concepts such as social constructionism, which argues that humans create subjective interpretations of their social reality. In contrast subjects aligned with technology and engineering could be argued to take a more positivist approach, in which there is an assumption that there is an objectively correct explanation for any phenomena. When educating cyber security students about psychology it is important to have an appreciation of these differences.

Drawing upon our own interdisciplinary activities to deliver psychology content as part of cyber security education and training programs this paper will explore and discuss two topics. Firstly, we will identify the areas of psychology that, based on our own experiences, is likely to be the most useful and relevant to cyber security students. Secondly, we will suggest how best to address the ontological and epistemological differences in approaches that may arise in psychology and cyber security education and training activities.

2 Identifying Relevant Areas of Psychology

Psychology is a broad discipline, with many areas of research that could potentially be pertinent to a complex and multi-faceted issue such as cyber security. To identify areas which are the most important we consider the issue in terms of understanding both the cyber adversaries and their targets.

2.1 The adversaries

A common form of psychological manipulation used by cyber attackers is social engineering, exemplified by phishing emails. Whilst the stereotypical phishing email is characterized by poor grammar and often crude attempts at manipulation it has been noted that these are becoming increasingly sophisticated and persuasive [3], with the most convincing tricking users up to 45% of the time [4]. These phishing emails exploit the decision-making heuristics – mental short cuts – humans use as a necessity to navigate their complex environments and social worlds. An example of this would be use of a company logo within a phishing email in the hope that the recipient will use the presence of this an indicator that the email is genuine. Other psychological processes relevant to phishing include Protection Motivation Theory [5], in which a fear appeal (e.g. a phishing email falsely claiming that a bank account has been hacked) is used to motivate a user into taking actions that put themselves at risk. However, not all of the processes cited by social engineers are supported by psychological research. For instance neuro-linguistic programming has been listed by some social engineers as an effective technique [6], but is largely considered a pseudo-science by psychologists [7]. This demonstrates the importance of evidence based, psychologically informed cyber security education.

Adversaries' common psychological patterns may help in recognizing threats. There are many forums and website on which individuals discuss cyber security attacks, both actual and hypothetical. It has been noted through analysis of these discussions and chat logs that cyber adversaries often appear to display cognitive dissonance over their actions. This refers to the discomfort felt by individuals when they have two contradictory beliefs or values. Regardless of how dismissive an individual cyber attacker may be of

their targeted victim they are still likely to feel at least a degree of guilt over causing harm to others. Rogers [8] notes that cyber attackers engage in various strategies to reduce cognitive dissonance. This includes the use of euphemistic language; blaming their actions on social pressures whilst minimizing their own individual roles in group-based actions; minimizing the negative consequences of their actions; and vilifying and dehumanizing their targets. Awareness of these processes may help cyber security practitioners better review possible threats, and also aide them in differentiating an actual, imminent threat from idle chat.

Another important area of psychology in relation to cyber adversaries is motivation and group identity [30]. Various typologies of adversaries have been proposed, including Seebruck's circular order circumplex model [9], which divides hackers into those motivated by prestige, recreation, revenge, profit and ideology. An awareness of these varying motivations is important for cybersecurity students, as this will improve their understanding of the behavioural patterns and possible future actions on adversaries. For example, the motivations and actions of a hacktivist group using a distributed denial of service attack to make an ideological protest against an organisation are different from those who are financially motivated. This is linked to group processes. It is of course often difficult to attribute blame in the case of many cyber security incidents, but several of the more high profile cases that have been investigated in depth have contained a group element [10, 30]. It is known from social psychological research that being part of a group alters an individual's behaviour and cognition in a number of ways, although we are often unaware of the degree to which the membership of the group is influencing us [11]. This includes cognitive biases which lead them to overestimate the ability of their own group, whilst underestimating the skill level of their opponents, as well as making riskier and more extreme decisions than would be the case if the individual acted alone [12]. An awareness that cyber adversaries are acting as a group can also be used to inform how best to publicly respond to the attack. As suggested by the category differentiation model [13] an external party identifying a group as a group reinforces their sense of group cohesion, which may in turn make further actions and attacks more likely Such a processes is argued to have been evident in relation to the hacktivist collective Anonymous, where media reports of their activities emboldened the group and reinforced their sense of group identity [10]. By having an awareness of these group processes cybersecurity students may again be better placed to better predict the future behaviour of cyber adversaries.

2.2 The Targets

Cyber security attacks that involve a human element often rely upon the target performing, or failing to perform, certain behavioural actions. By examining demographic factors and individual differences it may be possible to identify which individuals are at particular risk. As has been demonstrated by such research those who are most at risk may not match popular stereotypes of vulnerable computer users. For instance, it has been observed that younger adults may be at greater risk at being tricked by phishing

emails, despite their presumed greater familiarity with internet technologies than older adults [14]. This is related to the cognitive biases that individual may demonstrate in relation to their cyber security behaviors, with for instance individuals being shown to ignore warnings about risks if they are confident in their ability to minimize the consequences of a security breach [15]. In addition, there is evidence that people do not change their use of social network sites, even if they have previously been hacked [16]. Organisations have also not been found to change their security practices post breach or they make only a few modifications with the belief that these changes shield them from future attacks [31]. There is little understanding that threat vectors change and evolve often becoming more sophisticated and difficult to detect [31]. This may reflect the privacy paradox [17], in which individuals are motivated to maintain their reputation and identity online, even at the cost of taking actions to protect themselves. Further cognitive biases include exaggerating unusual risks whilst downplaying more common risks; underestimating risks that fall under the individuals remit whilst overestimating risks outside their control; perceiving personified risks to be greater than anonymous risks; believing themselves to be at less risk than their peers; and finally overestimating risks that may become a focus of public discussion [18, 19].

It is important to note that these cognitive biases do serve an evolutionary function. As discussed by Kahneman [20], cognitive biases and other forms of decision making heuristics are necessary as it would not otherwise be possible for us to process the vast amount of information that we are continually encountering. In other words, while ideally we would approach every situation with thorough, comprehensive consideration, the cognitive demands of doing so would be too great. Instead, we must make use of heuristics and biases to come to quick decisions, often based on relatively limited information. The tendency of people to do so can easily create frustrations for cyber security practitioners, who would prefer users to be approaching any situation relating to cyber security with the slower, more considered approach. Successful social engineering strategies are often based on encouraging targets to engage in the quicker form of decision making, which is why for instance many phishing emails will include a fear appeal or an element or urgency. Many attempts to promote positive cyber security behaviors in the workplace aim to encourage users to always be taking the slower, more thorough approach to cyber security related activities, rather than making quicker decisions based on a smaller number of cues. Yet psychologists would argue that this is not sustainable; and that it is important to accept that the tendency of humans to make quick decisions is an evolutionary need, not an inherent design flaw. By better understanding how humans make decisions, cyber security practitioners may be better placed to determine how to design systems that take these factors into account.

As with cyber adversaries, the individuals who are targeted in cyber-attacks are also often part of groups. These social influences need to be acknowledged when considering cyber security behaviours, that is how group processes may hinder or help when cyber security processes and policies are being implemented. For example, as based on the Theory of Planned Behaviour it has been noted that the intention someone has to perform a desired behaviour (such as updating software) is in part determined by

whether they think influential others will support or condemn their actions [21]. For instance, the IT department of a company may direct all staff members to take actions to ensure that the software on their PCs is up to date, but if an individual user is concerned that their immediate manager will be unhappy about the downtime this will cause then they will be less likely to follow these actions. Social interactions and interpersonal relationships are also factors relating to insider threat, both intentional and unintentional. Band et al [22] identify several relevant factors, including stressful events observable in personal and work life, and stressful events in relation to the workplace, including conflicts and sanctions. These factors are of course highly psychological in nature, and making use of pre-existing psychological educational materials could help educate cyber security students on how to identify and measure key psychosocial factors.

3 Pedagogical Approaches

Successfully incorporating psychology into cyber security education relies not just on identify what information should be delivered, but also how it should be delivered. It is important to acknowledge that cyber security students and training course attendees will often have a certain perception of what psychology entails. A common perception we encounter is that psychology is only concerned with mental illness, and that the methods that are used are highly personal and subjective. It can come as a surprise to cyber security students that psychology as an academic discipline is far broader, and in many countries, will only be offered as a science degree (e.g. a Bachelor of Science in the UK, as opposed to a Bachelor of Arts). As discussed in Taylor [23], there are important differences in ontology and epistemology between psychology and computing-related disciplines, which shape how students view the world and how receptive they may or may not be to different educational approaches. In this section, we will review our experiences teaching psychological principles to cyber security students and practitioners across a range of settings. This includes undergraduate and postgraduate courses, short courses for continuing professional development and training packages for commercial and industrial partners.

3.1 Understanding Student Motivations and Expectations

Students undertaking some form of cyber security education or training can come from varied backgrounds, including those entering university or colleges course directly from school and those who are already working in industry. Differences between reasons why students chose computing and psychology degrees has been investigated by a number of psychologists. For example, it has been found [24] that computing students were primarily interested in developing problem-solving and logical thinking

skills, as well as increasing future earning potential. Psychology students on the other hand placed more emphasis on understanding other people, oneself and developing greater personal independence. In addition, and perhaps not surprisingly, psychology students also expressed greater interest in understanding social relationship and interacting with people, whereas computing students were more interested in understanding and interacting with technological systems. It is important to take these differences into account when planning and delivering cyber security education and training. This relates not to just to the academic background of the individual, but also their level of maturity and life experiences. In our experience younger undergraduate students from both psychology and computing backgrounds appear to feel less equipped to discuss the moral, ethical and philosophical issues that arise in cyber security. Gibb et al observe that undergraduates' may not have yet fully developed their understanding of how moral issues relate to societal functioning [25]. Therefore, cyber security education may need to be tailored towards the student population to whom the material is being delivered.

It is also important to recognize that students studying for cybersecurity courses are likely to have been taught in different ways and may approach studying in different ways, compared to those studying for psychology degrees. On the one hand, based on our own experience computing assignments tend to require answers that are unequivocally right or wrong, or at least where there is finite set of correct solutions. Within psychology, on the other hand, the emphasis can often be on the quality of the debate that is put forward by the student, with there often being no correct answer. This is not of course the case with all areas of psychology – in some sub-disciplines such as neuropsychology for instance there is a clearer sense of information being either right or wrong, which is in keeping with such sub-disciplines being considered more 'scientific' than other areas of psychology. Nevertheless, we would argue that there is a greater emphasis in psychology on an objective evaluation of theories, whereas assignment in computing tend to have a more problem-solving focus, which solutions or answers deemed to be either correct or incorrect. Depending on their background it has also been our experience that cybersecurity students can find the methodological approaches used in psychology to be quite different from what they have previously experienced. An experience we often have when we presented multiple (occasionally contradictory) theories to cyber security students is to be asked which theory is the correct one – they are then often surprised, and at times frustrated, when we reply there is no single, universally accepted theory which is seen as the correct one.

3.2 Perspective Shifting

It has been our experience that cyber security students tend to focus on how the actions of the target enabled or facilitated the cyber-attack. However, in our experience it seems that while students are interested in the how and the what, they are less interested in the why. Similarly, cyber adversaries tend not to be considered,

beyond an analysis of what their actions were. In the sessions we have delivered with cyber security students we have attempted to promote a deeper understanding of the psychological processes displayed by both the targets and the cyber adversaries. One way we do this is by asking the students to consider the incident from the perspective of both parties. For example, students are asked to identify high risk group and to consider how advice should be tailored to that group so that it will be understood and acted upon. They are then asked to design a cyberattack that would circumnavigate their own advice, again taking into account the psychological characteristics of the target group. In doing so students are encouraged to think about the various psychological processes discussed in Section 2, and to develop a deeper understanding of why adversaries may have chosen a target, why they chose a particular attack methodology and why the targets may have failed to identify and mitigate the attack.

Another instance where we extended a two-way relationship between psychology and cyber security is during the teaching of digital investigations and forensics. The processes of cyber forensic analysis function in a complex problem space, due to the increased uncertainty surrounding forensics investigations in general. Since digital investigations refer to an activity related to an individual or a group of cyber criminals, an understanding of psychology plays a significant role. For example, if when deciphering the evidence files an exhaustive search becomes the final option (due to failure of all cryptanalytic attacks), the data would need to be decrypted based on constructing case-specific dictionaries according to the psychology of the suspect's behaviour. In such cases, behavioural profiling is used to identify certain traits, preferences or tastes of the suspect that can assist in constructing a collection of dictionaries of passwords. These shifts to employing psychological perspectives in the analysis of digital evidence also contributes to the understanding of the socio-psychological behaviour of cyber criminals. Moreover, it was found that integrating psychology and digital investigations and forensics on an epistemological level not only resulted in added value for the cyber security students, but also of paramount importance that cyber security involves psychology in order to compensate for the significant uncertainty that governs the analysis of cybercrime.

Finally, cyber security students—and their professional counterparts—often approach cyber security concerns with the addition of new systems; adding authentication requirements, password requirements, policies, and permissions restrictions. But these approaches often add complexity to an already complex operations ecosystem, make the work of the employees more arduous, and rarely patch the true causes of the security gaps. The types of evidence-based design principles offered by the user-design field of psychology helps cyber security students better understand the need for usable security systems—systems that improve security and reduce potential loss where employees do not feel overburdened—and how to implement them. Usually, the goal is clarity for the user, but user design can also be used to add desirable difficulties for end-users [26]. Desirable difficulties, or a marker that breaks up the flow of current activities, can be used as a tool for increasing awareness at key times [27]. Teaching cyber security students about usable design, and more specifically usable security, allows them to consider new approaches to cyber security that account for the ways in which their staff will interact with the systems they create.

3. Teaching Psychology in the Workplace

Many of the learning outcomes emerging from teaching psychology and cybersecurity are now being used as the basis for commercial tools that can be used to address cyber security practice within organization. However, there are important differences in context between a college and university course and the work place. Cyber security students may be skeptical about the role of psychology, but it is reasonable to assume that they do at least have an interest in cyber security overall. As such the main challenge is to demonstrate to them why psychology is an important topic in relation to cyber security. In organisations however, users may not have initial interest in cyber security at all. Even if they do there may be greater pressures of time and money within a workplace, that mean that cyber security education has to be delivered in a much shorter time scale. The academic authors of this paper have explored these challenges in conjunction with practitioners.

In the UK, we have worked with LiMETOOLS, a highly specialised publisher of learning tools that bring about behavioural change in areas of high commercial risk management, including cyber security. Making use of social cognitive learning theory [28] employees are prompted to consider how behavioural actions may lead to and facilitate cyber security attacks way similar to the perspective taking exercises used with students. Interactive dramas are used immerse learners in examples of realistic cyber security incidents, followed by interactive quizzes to assess knowledge. A tool targeted at graduate workers who used social networks heavily has also been created. As such rather than attempting to cover the full range of possible cyber security risks the tool focuses on a key area that is often utilized by social engineers. The tool exposes a fictional hacker at work, whilst facilitating the learner through a process creating their own action plan. On the basis that prevention is better than cure a second tool offers graduate recruiters an audit tool for new potential employees to calculate their vulnerability in the cyber domains relevant to a wide range of industrial sectors. As such the tool both educates and audits at the same time.

Further prevailing methods used by organisations in Australia involving psychology to address cyber security risks are centered on HATCH Training (Hacking and Tricking Capricious Humans) using real time scenarios to help employees learn different cyber-attack situations and the processes to tackle them. This method particularly has been found effective in reducing phishing, ransomware, physical manipulations, and spear phishing related attacks. In addition, simulation-based training using gamification tools where live examples are presented along with solutions is now commonly applied by large organisations. The gamification aspects of the training are focused on assessing the behaviour of hypothetical victims of cyber-attacks through psychological manipulations. This was observed to have a major impact on increasing the level of cyber security risks awareness among employees. Besides, some well-resourced organisations

now find it crucial to apply psychology to boost cyber security by targeting specific behavioural limitations such as cultural influence, biases, and cognitive preferences to identify noncompliant security behaviour of employees, as well as employees that are overestimating their capability to mitigate security risks. This strategy creates the possibility for organisations to design role-specific interventions for any identified weak points.

The key learning outcomes of these trials so far indicate six critical requirements for this kind of workplace learning that combines psychology and cyber security factors:

i) the immersive aspect of the approach through videos and dramatizations appear to be particularly effective with younger learners, who appear to be more easily distracted when less immersive teaching strategies are used;

ii) integrating well-executed and psychologically backed game design with intellectual challenges, and positive reinforcement techniques improves learner's engagement, thus, promoting behaviour change and knowledge retention;

iii) learners demonstrated the wish to have control over their pace of learning and also the device on which they engage with the educational materials; this is consistent with psychological research that would suggest that giving people a feeling of control over their own behaviour change process is likely to improve outcomes [29];

iv) it is important to find a balance between the activities. Users respond best when there is a combination of videos, quizzes and interactive sessions. Users who did appear to find any one particular activity too extensive were observed to attempt to cheat the system to move to the next activity;

v) raising awareness is not by itself sufficient. Indeed, several users noted that after viewing the video materials they felt more nervous and uncertain than before about how to respond to cyber security threats. This relates to the aforementioned Protection Motivation Theory [16], in which individuals who are too afraid of a possible threat may not even attempt to avoid the threat, if they believe that such avoidance is not possible. The developer mitigates this risk by following up the input experience immediately with a module that supports the user in producing their own positive action plan to minimise the risk; and

vi) learners need to know how they are performing at regular intervals during the experience. The developer's Learning Management Software (LMS) is configured so that the learner can see their scores regularly and receive comparative data about their performance against the rest of their peer group. This can incentivise the enthusiasm for learning by itself.

4 Conclusions

We strongly believe that there is potential for the field of psychology to contribute to cyber security education and practice. To do so we need to consider which areas of psychological research are most pertinent to cyber security, whilst taking a pragmatic

approach that acknowledges the time and resources available when delivering cyber security education and training. We also need to acknowledge the differences in epistemological and ontological assumptions between psychology and cyber security students, and how these translate into teaching practice. By doing so we can work in an inter-disciplinary manner to better equip cyber security students and practitioners with the skills and knowledge they need to address cyber security challenges.

4. Brief Biographies of the Multidisciplinary Team

Dr. Jacqui Taylor-Jackson is Professor of Cyberpsychology in the School of Psychology at Western Sydney University. Jacqui is a psychologist who is passionate to engage and involve academics and students from computing-related disciplines in applying psychological research findings to understand and develop computing systems. Recently, she has been instrumental in the application of psychology theory and methods to cybersecurity teaching and learning, and has written several book chapters, journal articles and a white paper on this topic.
Jacqui is a Chartered Psychologist and Associate Fellow of the British Psychological Society (BPS), and she has held terms as Chair of the BPS Division of Academics, Researchers and Teachers in Psychology and Editor of the BPS publication *Psychology Teaching Review*. Jacqui is a Senior Fellow of the UK Higher Education Advance. Jacqui is currently President of the International Council of Psychology Educators. As part of these organisations Jacqui has organised symposia at International conferences relating to psychological literacy, online learning and teaching and the impacts of new technologies and ubiquitous connectivity on university students' psychosocial well-being. Jacqui's current research is evaluating and understanding the psychological impacts of technology and the internet on children and young people. For example, she has researched and reported on the wide-ranging positive and negative impacts of social media and videogames, in terms of sleep patterns, mental health issues, susceptibility to fake news, online moral reasoning and digital addiction.

Associate Professor John McAlaney is a Chartered Psychologist and Chartered Scientist, based within the Department of Psychology of the Faculty of Science and Technology. He completed his PhD at the University of West of Scotland, where he explored the social psychological factors associated with risky alcohol use. He has since expanded his research to include psychological determinants of other risk behaviours including gambling, digital addiction and cybersecurity. As part of this work he recently authored a briefing paper for the British Psychological Society that set out the position of the Society in the role of psychology in the development of cybersecurity capabilities in the UK. He has secured funding in the form of grants and several match-funded PhD studentships to further develop this area. John applies this research to real-world problems through his role as a Trustee of both the Gordon Moody Association; a residential service for problem gamblers, and Acts Fast; a charity which supports protective parents and family members of children who have been sexually abused.

Dr. Jeffrey Foster is Senior Lecturer of Online Social and Behavioural Sciences at Western Sydney University's School of Psychology. He completed his PhD in cognitive Psychology at the Victoria University of Wellington in New Zealand in 2013, and a postdoctoral research fellowship examining the relationships between intelligence and executive functioning at the Georgia Institute of Technology. Broadly speaking, his research focuses on the applied aspects of Human memory and cognition - particularly as it applies to security and the court room. Dr. Foster has been funded by the New South Wales Cyber Security Network and the Australian Defence Forces, and has previously worked with both US Defence and Intelligence agencies in measuring cognitive abilities to predict task performance.

Dr Abubakar Bello is Course Leader and Lecturer in Cyber Security and Behaviour at the School of Social Sciences: Criminology and Policing discipline, Western Sydney University. He received his doctorate degree in IT with a technical, business and social focus on Information Security and Privacy from Murdoch University, MBA from Western Sydney University, and MSc and BSc in Computer Science from the University of Wolverhampton UK. He has extensive teaching experience ranging across various information systems, cyber security and risk management courses, and also worked across several corporations, privately held entities and government organisations in Australia where he provided technology audit and security risk management services. He is currently researching on Active Cyber Defence Security Strategies (ACDS) for fighting cyber-crime; and the role of cyber security controls on people performance and satisfaction. He also has a strong interest in conducting research in areas such as security in social networks, security predictive analytics, cyber physical systems, security and dependability, business applications, trust, privacy, cyber forensics, cyber security risks and decision making, and the psychology of security compliance in the cyber space. Abubakar is a member of professional and academic computing society bodies, and has been an ad hoc reviewer of academic journals.

Dr. Alana Maurushat, is Professor of Cybersecurity and Behaviour at Western Sydney University where she holds a joint position in the School of Computer Data & Math Sciences and in the School of Social Sciences, and is Key Researcher with the CRC Smart Satellites. She is currently researching on payment diversion fraud and ransomware, neural network spiking anomaly detection, tracking money-Laundering through bitcoin blenders, distributed extreme edge computing for micro-clustered satellites, and ethical hacking. She previously was Senior Lecturer in Law, Key Researcher on the CRC Data to Decisions – Big Data in National Security, and Senior Fellow with the Australian Cybersecurity Centre for Research and Education all at UNSW. She is the Cyber-Ambassador for the NSW Cybersecurity Network. She is on the Board of Directors for the cybercrime investigation company IFW Global where she provides special advice for specific cybercrime investigations involving organised criminal syndicates. She lectures & researches in Cybersecurity, Privacy and Security by Design, Cyber Risk Management, and Artificial Intelligence across the disciplines of Law, Criminology, Business, Political Science and Information Communications Technology. Alana has done consultancy work on Cyber Security, Open Data, Big Data, Technology and Civil Liberties for both the Australian and Canadian governments, industry

and NGOs. Alana regularly engages with the media (e.g. 60 Minutes, the New York Times, Insight, ABC, and 730 Report) and is the author of many books and articles.

Dr John Dale has led organisations in media production for over 30 years, including senior creative and managerial roles in the BBC and the UK's main commercial channel, ITV. John is a co-founder and Executive Director of Products & Services of LiMETOOLS, a corporate online training provider using interactive rich media to support large business behaviour change related to Cyber Security. He is also a Director of Silicon South, a development agency for creative digital companies in the south of the UK and a Trustee of EXplora, a children's science and engineering attraction and a STEM online gaming experience. John is uniquely able to take the scientific and technological facts of the changing world and blend them into compelling storytelling that can be used by business and policy makers to enhance and promote their understanding of the future and assist in behaviour change.

References

1. Dawson, J., Thomson, R., *The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance*, Frontiers in Psychology, 2018, 9, 1664-1078. Available from https://www.frontiersin.org/article/10.3389/fpsyg.2018.00744
2. Kearney, W.D. and H.A. Kruger, *Can perceptual differences account for enigmatic information security behaviour in an organisation?* Computers & Security, 2016. 61: p. 46-58.
3. Iuga, C., J.R.C. Nurse, and A. Erola, *Baiting the hook: factors impacting susceptibility to phishing attacks.* Human-centric Computing and Information Sciences, 2016. 6(1): p. 8.
4. Bursztein, E., et al., *Handcrafted fraud and extortion: Manual account hijacking in the wild*, in *Proceedings of the 2014 Conference on Internet Measurement Conference*. 2014, ACM: Vancouver, BC, Canada. p. 347-358.
5. Johnston, A.C., M. Warkentin, and M. Siponen, *An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric.* Mis Quarterly, 2015. 39(1): p. 113-134.
6. Hadnagy, C., *Social Engineering: The Act of Human Hacking*. 2011, Indianapolis: Wiley Publishing Inc.
7. Witkowski, T., *Thirty-five years of research on neuro-linguistic programming. NLP research data base. State of the art or pseudoscientific decoration?*, in *Polish Psychological Bulletin*. 2010. p. 58.
8. Rogers, M.K., *The psyche of cybercriminals: A psycho-social perspective*, in *Cybercrimes: A Multidisciplinary Analysis*, G. Ghosh and E. Turrini, Editors. 2010.

9. Seebruck, R., *A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model.* Digital Investigation, 2015. **14**: p. 36-45.
10. Olson, P., *We Are Anonymous*. 2012, New York: Back Bay Books.
11. Darley, J.M., *Social organization for the production of evil.* Psychological Inquiry, 1992. 3(2): p. 199-218.
12. Wallach, M.A., N. Kogan, and D.J. Bem, *Group influence on individual risk-taking.* Journal of Abnormal Psychology, 1962. 65(2): p. 75-&.
13. Doise, W., *Groups and individuals: Explanations in social psychology*. 1978, Cambridge: Cambridge University Press.
14. Sheng, S., et al., *Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions*, in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2010, ACM: Atlanta, Georgia, USA. p. 373-382.
15. Rifon, N.J., R. LaRose, and S.M. Choi, *Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures.* Journal of Consumer Affairs, 2005. 39(2): p. 339-362.
16. O'Connell, R. and G. Kirwan, *Protection Motivation Theory and online activities*, in *Cyberpsychology and New Media: A Thematic Reader*, A. Power and G. Kirwan, Editors. 2014, Psychology Press: New York.
17. Utz, S. and N. Kramer, *The privacy paradox on social network sites revisted: The role of individual characteristics and group norms.* Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 2009. **3**(2).
18. Schmidt, M.B. and K.P. Arnett, *Spyware: A little knowledge is a wonderful thing.* Communications of the Acm, 2005. 48(8): p. 67-70.
19. Schneier, B. *The Psychology of Security*. in *First International Conference on Cryptology in Africa*. 2008. Casablanca, Morocco: Lecture Notes in Computer Science.
20. Kahneman, D., *Thinking, fast and slow*. 1st ed. 2011: Penguin. 499 pages.
21. Venkatesh, V., et al., *User acceptance of information technology: Toward a unified view.* Mis Quarterly, 2003. 27(3): p. 425-478.
22. Band, S.R., et al., *Comparing insider it sabotage and espionage: A model-based analysis*. 2006, Software Engineer Institute, Carnegie Mellon.
23. Radford, J. and L. Holdstock, *Gender differences in higher education aims between computing and psychology students.* Research in Science & Technological Education, 1995. 13(2): p. 163-176.
24. Taylor, J., Teaching psychology to computing students. *Psychology Teaching Review*, 2008, 14(1), 21-29.
25. Gibbs, J.C., *Moral Development and Reality: Beyond the Theories of Kohlberg and Hoffman*. 2003: SAGE Publications.
26. Bjork, E. L., & Bjork, R. A., Making things hard on yourself, but in a good way: Creating desirable difficulties to enhance learning. Psychology and the real world, 2011, *Essays illustrating fundamental contributions to society*, 2(59-68)

27. Linn, M. C., Chang, H. Y., Chiu, J., Zhang, H., & McElhaney, K., Can desirable difficulties overcome deceptive clarity in scientific visualizations, 2011, In A. S. Benjamin, *Successful remembering and successful forgetting: A Festschrift in honor of Robert A. Bjork*, 239-262 Taylor & Francis. https://doi.org/10.4324/9780203842539
28. Bandura, A., *Social cognitive theory*, in *An Introduction to the Theories of Personality*, R.B. Ewen, Editor. 2003, Lawrence Erlbraun Associates: Mahwa. p. 365 - 386.
29. Steptoe, A. and J. Wardle, *Locus of control and health behaviour revisited: a multivariate analysis of young adults from 18 countries.* Br J Psychol, 2001. 92(Pt 4): p. 659-72.
30. Maurushat, A., *Ethical Hacking.* University of Ottawa Press (2019).
31. Maurushat, A., Bello, A. and Bragg, B., Artificial Intelligence Enabled Cyber Fraud: A Detailed Look into Payment Diversion Fraud and Ransomeware, Indian Journal of Law and Technology, forthcoming (2019).

.