Foreword

Introductions to books such as this one very often include proclamations that "this is a timely volume", to the extent that the phrase becomes something of a cliché. In this case, however, it is absolutely true. The themes and topics covered by this book bear directly on our understanding of, and reactions to, events that have an ongoing, significant and sustained impact on the world in which we live.

Formal definitions of 'cyber security' typically revolve around systems, standards, technologies and processes for protecting computer systems, networks and the data they contain from unauthorised access or malicious attacks. Such a definition may imply that cyber security is somewhat of a dry, technically focused enterprise, mainly of concern to computer scientists and industry professionals. That is a long way from the truth: cyber security, and security violations, have profound implications for all of us.

We now live in a world where all manner of devices, services and the people who use them are networked and vulnerable to electronic attack. These range from obvious targets like traditional computer and telecommunications systems, to nuclear reactors, children's toys and domestic appliances. All may be threatened or exploited in different ways. As our reliance on communication technologies and networked devices inexorably grows, cyber security will become more and more critical to society.

At the time when this book was being written, various aspects of cyber security were rarely far from the headlines. Businesses and public services including hospitals, were crippled by ransomware attacks. Online fraud was rampant, with costs to economies and individuals that are hard to quantify. In a number of countries, there were allegations that foreign states had hacked political campaign organisations, resulting in the theft and publication of emails for political purposes. There were accusations of meddling in multiple elections by electronic means. There were frequent concerns about online influence leading to political and religious extremism, and the use of telecommunications and networks by terrorists, criminals and national security agencies. Loss, theft, and publication of personal information were depressingly frequent, ranging from the personal photos of celebrities to very large scale losses of personal data and breaches of confidentiality by public and private organisations. Whether directly or indirectly, issues such as these touched all of our lives.

In any technical field, there is a tendency to prioritise technical approaches to solving problems. However, hardware and software engineering can only ever be part of the solution to cyber security. Since the days of the earliest computer hackers, it has been known that the human element is among the weakest components in any system. The use of 'social engineering' techniques (manipulating people in various ways to gain access to secure computer systems) was, and remains, a key weapon in the arsenal of those who seek to illegitimately access or attack the systems, services and infrastructure underpinning many aspects of modern life.

Humans will always interact with any information system at some level, and human behaviour thus becomes a part of the system. And of course, a human actor is always the instigator of any attack upon a system. It is therefore imperative to understand how people interact with the technologies at hand, and what individual behaviours may introduce vulnerabilities. For example, what factors might make some individuals or organisations more susceptible to malicious influence? How do psychological phenomena and information technologies mediate, underpin or facilitate such processes of influence? What can be done to protect individuals, groups and systems from such attacks? These questions are clearly in the domain of psychology and the behavioural sciences. Without considering them, no approach to cyber security can ever be successful.

This collection of chapters deals with several key themes around the intersection of psychology and cyber security. One of the areas explored is individual decision making in online environments, which leads to the considerations of privacy protection behaviour, trust formation and individual cyber security concerns affecting consumer behaviour and ultimately victimisation. Next, a number of phenomena relevant to cyber security on a global level are addressed. In particular, this volume investigates how culture and religion might impact upon security, arguing that cyber security measures and technology acceptance are affected by individual cultural differences. The discussion delves into the issues connected to online radicalisation and cyber terrorism reflecting the currency of this volume in light of the recent attacks worldwide and the pressing need to bring this phenomenon to an end. Cyber security professionals often say that we can never achieve a perfect cyber security posture. The risk of cyber security threats rather is said to be minimised through the application of protective mechanisms and security controls. The discussion of cyber security will not be complete without addressing two key elements in this: how can we educate and motivate individuals to behave in a way that reduces risk?

Drawing on up-to-date research findings, each chapter addresses key practical and theoretical issues in a variety of important applied contexts. The questions addressed here are not just of academic interest; they have critical implications for the security of our society. Taken together, these chapters provide an excellent overview of current research and thinking across a broad spectrum of cyber security-related issues and behavioural phenomena. They will prove a valuable resource both for those working in the behavioural sciences, and those with a more technical focus. It is only by different disciplines working together across that boundary that risk can be reduced and security enhanced.

Tom Buchanan
University of Westminster, UK

Preface

Researchers in a variety of disciplines turn to psychology to help understand human behaviour and decision making. Psychology has a long history of understanding human behaviour, thoughts and actions. By applying that research and theoretical knowledge to the topic of cyber security, academics and practitioners may be able to better understand why and when people engage in cyberattacks. Such knowledge is useful to those in law enforcement and policy. It is also crucial to those working in organisations who try to keep their companies safe.

Threats can come from inside the organisation or from outside. Insider threats pose a particularly difficult challenge as one has to monitor who may be a threat and to some extent why they are a threat at any given time. To know that, we must rely on psychology to help us analyse human behaviour. Without a foundation in how to better understand human behaviour, we could be at a loss to predict who may be an inside threat.

Outside threats are in some ways easier to understand and many cyber threats originating outside an organisation require no assistance from insiders. There is only so much technology can do to keep corporations safe. As good as the technology is, humans are adept thinkers and will be able to navigate a way around most security systems. That is not to say that anyone could do so, but those who have a knack for it and are so inclined could breach the security. Those who are less skilled but equally as motivated, may be able to pay someone to breach the organisation's security.

Concepts such as trust and relationship development are relevant to this work. Psychology has long studied these ideas and can contribute a significant literature to them. For example, in trust studies, psychological research has investigated how the concept is developed, and how it is fostered. It looks at what leads to a breakdown in trust in dyads as well as in larger group settings. Through this sort of research, we may be able to apply it and develop a greater understanding towards how hacking groups are formed and rely on each other to breach a security wall. We may also use it to try to mitigate such violations by developing interventions to build trust within an organisation or between the organisation and potential outside hackers.

Similarly, we may rely on psychological research in relationship development. We could look at how relationships are created and who wants to be part of certain relationships. We could look for weaknesses in relationships and what holds people together. Understanding why certain people are drawn to others, what motivates groups to form and to have a particular agenda, is all crucial in considering security of cyber systems.

Aspects of disinhibition and anonymity in the online setting need to be considered as well. Disinhibition has been studied in psychology since at least the 1960s. Addressing what increases people's chances of acting in a particular circumstance or failing to act in others is not new to the field. What

is new, however, is looking to see how that research and those findings may be applied to the online environment. What features about individual differences may increase someone's chances of using the internet to engage or encourage terrorism? What might make an individual think about why s/he should use online media for a social protest or choose to protest in a more traditional way, or not at all? Theories and research in social psychology have studied why people may be inhibited or disinhibited to act in certain ways; these book chapters are able to use that foundation as a cornerstone to better explore how the human agent is relevant in cyber security.

Anonymity is an interesting concept to consider both in psychology and cyber security. We know from psychology that in large groups when people feel that they cannot be identified (that is, they are anonymous) they are more likely to engage in risky behaviour. It is possible, therefore, that we would expect that sort of behaviour in the online environment where identity may be protected. The importance of this to cyber security is not to be considered lightly. If techno-savvy people can protect their identity, this leaves a vulnerable online environment rife for infiltration. Infiltration could come from multiple sources as many of these chapters attest to. The insider threat, especially if the culprit could remain anonymous, is undoubtedly of concern. The hackers or those who are simply interested in breaching cyber security for the thrill of it with low risk of getting caught may feel a challenge waiting. Engaging in social protest again with a low cost as the methods of finding the perpetrator are not well established could lead to those with only minor grievances to consider violating the security wall. More structured groups who wish to see a corporation's downfall are able to spend the time, effort and energy to develop a well-planned security breach. They may be able to call on outsiders to help, again as the prospect of remaining unknown is substantial.

Ethics is another area where psychology has spent a fair amount of time trying to consider how to understand human behaviour from a theoretical perspective whilst also ensuring that human rights are not violated. In doing so it provides a good cornerstone to address cyber security from multiple angles. First, by considering the research that has been done to understand human behaviour, someone looking at violations of cyber security can rely on solid design with ethical guidelines fully considered. From the organisation's viewpoint, second, a foundation in psychology can help to guide strict approaches to prevent breaches while still mainly an ethically appropriate approach to employees and those who use and interact with the organisation. Third, company may consider, again ethically, how to prevent security breaches whilst maintaining a usable online platform.

Using these concepts as well as other aspects that are cornerstones of psychological research we can see how it is a crucial field to consider when looking at cyber security. Human behaviour is at fault for a number of security violations, especially if the technology becomes more and more robust. Relying on well evidenced and well researched concepts within human behaviour, we see how the human element is a base to understand and mitigate intrusions in cyber security.

This book covers a variety of topics and addresses different challenges that have emerged in response to changes in the ways in which it is possible to study various areas of decision making, behaviour and human interaction in relation to cyber security.

Each of the chapters brings its own contribution on how psychology furthers our understanding of cyber security. The innovative chapters link a strong foundation in human behaviour research with application to a topic of crucial importance in today's world. By looking at the chapters (see descriptions below) it should be clear how this topic is of the utmost importance in today's world. Understanding

cyber security and breaches in it can only help to make all of us safer. Looking at ways to protect our finances, our images stored online and companies protected data, helps us all. Considering research on psychology and cultural identity may help us in understanding who and in what circumstances someone may decide to encroach on secure systems.

In a world as complex and fast moving technologically as one in which we find ourselves, a reference book such as this is a must. It provides the foundation of understanding aspects of human behaviour coupled with an area of real concern criminologically. It is necessary at this juncture of technology and human behaviour to understand who, when and why people might breach security systems. Who are the players most likely to do this and what can the authorities, policymakers and organisations themselves do to mitigate these threats? When are breaches likely to take place? Does it happen when political tensions rise and those prone to engaging in terrorism might increase? Does it happen when employees become disgruntled? How about when people want to set themselves a challenge to see if they can violate a security system? There are numerous questions about why these intrusions may happen at this particular time and in particular places. Culture, decision making, spotting vulnerabilities, etc. all make for an online system that is rife to be breached. In today's society, we cannot take a lax approach to our security nor to leaving human behaviour to the academics. We must join forces to make sure that we all stay safe, and continue to understand, before the violators do, what cyber vulnerabilities we have exposed.

This book was written with a large audience in mind. First, it was created for the practitioner. When understanding your own organisation and how to protect it, we thought a base in human behaviour would be relevant. If human behaviour and a century of research in this field is ignored, we are not using our collective knowledge to help society today.

Second, this book is addressed to the policymaker. Knowing what the risks are from the organisational perspective interwoven with research is crucial when considering applications of academe. Policymakers often do not have the luxury of reading the latest research in a field before needing to consider the political agenda. Hopefully this book gives a summary of relevant literature when contemplating cyber security.

Third, this book was conceived for the academic and researcher. These chapters show how theoretical work in psychology can be applied to a timely and real world problem. As much as researchers enjoy studying concepts to support or refute theory, to do so and see it have great impact in the broader community is pleasing. This book exemplifies how such work can provide said impact. Reading the chapters provides a trail map of concepts in psychology being applied to keeping us all safe in the cyberworld.

Finally, technology developers should read this book. Those who work in the field of cyber security undeniably see the thin line that is walked between staying secure and keeping cyber systems free. We all want systems that allow as many people to use them as possible and to keep our lives as simple as they can be. But, creating a banking system for people to use from the comfort of their home, while it may keep our lives simpler as we do not need to go to the bank during opening hours, is not useful if our finances are at risk. A fine balance must be found by our technology counterparts to ensure that social groups may use online fora without posing a risk for terrorist attacks. If the technologists can find that happy medium, we are in as safe and user friendly a world as possible. The problem of course is that that line often moves and the technologists may use this book to better understand how human behaviour can change and shift over time, providing them a stronger foundation for which to understand where that line is moving to next.

Below is a brief summary of the chapters in this book. They range across topics as you will see but hopefully gives a flavour of how psychology can contribute to this field. As both psychology and cyber

security are vast, it does not attempt to be an exhaustive book. Yet, it should give a strong foundation on understanding a range of relevant topics from decision making, cognitive bias, terrorism, social media and guidance on how to do one's own study in an ethically appropriate way.

Chapter 1, "Online Decision Making: Online Influence and Implications for Cyber Security," addresses the challenges of understanding the differences between decision making that is performed online and research that uses an online forum alone. This chapter looks at how computer mediated communication impacts on how we make decisions online. Developing perspectives on decision making, and the applicability of the theories to the online environment is considered, with issues such as buying behaviour to radicalisation being addressed. This chapter encourages joint thinking from the practitioner and the researcher. It offers the idea that multiple models and perspectives are needed to understand how CMC influences our capacity to make decisions in the online forums.

Chapter 2, "Human Factors Leading to Online Fraud Victimisation: Literature Review and Exploring the Role of Personality Traits," highlights the role human behaviour has as the weakest link in cyber security. This literature review explores the role of personality traits, seeks an explanation for online fraud victimisation, and does so from a criminological and psychological perspective. First, a review of the literature in this area is presented. More specifically, the routine activity approach and the Big Five personality traits are discussed and applied to online fraud. Second, a novel empirical study on personality traits is presented, in which the influence of the Big Five personality traits on online fraud victimisation is assessed. This chapter ends by presenting implications for online fraud prevention as well as possibilities to advance the study of cyber victimisation.

Chapter 3, "The 'Human Factor' in Cyber Security: Exploring the Accidental Insider," describes the threat posed by members of an organisation. These threats may come from disgruntled employees or more innocuously from ignorance. Either way, they pose a potentially serious threat to information security. This chapter discussing aspects of the insider threat as well as the human factors that may contribute to one becoming a threat. Methods to detect and mitigate the threats are presented here.

Chapter 4, "Cyber + Culture: Exploring the Relationship," highlights some of the findings of a selection of recent studies on the relationship between national culture and specific cyber behaviours. The goal of this work was to understand the ongoing problem of attribution in cyber security as advances in technology is showing improvement in cyber-attack attribution, albeit slowly. Interest in the psychological research of decision making and the role of the human in perception management lead to the belief that behaviour may be able to ward off some cyber-attacks by defending and training users. In modelling behaviours related to cyber security, one needs to consider the role of culture in values which shape behaviours. This chapter crucially contributes to an area of research that is lacking by providing foundational work in this field.

Chapter 5, "Examinations of Email Fraud Susceptibility: Perspectives From Academic Research and Industry Practice," covers issues associated with the positive and negative sides of the internet being used for entertainment, commerce and communication. The potential for human advancement in this venue is substantial but so is the risk of increasingly sophisticated cyber-attacks. These undoubtedly could have serious personal and commercial implications. From a psychological viewpoint the attacks offer an insight into the decision making processes which may lead to being a victim of online fraud. The authors use their chapter to attempt to understand responses to phishing emails whilst exploring how industry and academic research might collaborate to better address email fraud threats. Various methods to understand susceptibility and considering preventable security measures are used to try to develop integrative solutions.

Chapter 6, "Introducing Psychological Concepts and Methods to Cyber Security Students," discusses the role and impact of psychology research on cyber security education. By using both prior cross-disciplinary teaching experience and observations of teaching psychological principles and methods to undergraduate and postgraduate cyber security students, the authors have compiled information about their experiences. There is a strong focus on making the material accessible and engaging. Suggestions as to how to integrate psychological into the cyber security curriculum completes the chapter.

Chapter 7, "The Role of Psychology in Understanding Online Trust," addresses the challenges of trusting people in the online environment. The authors discuss the manipulation of trust and the sometimes dire economic and psychological consequences. Literature on developing trust online is reviewed and several case studies describe trust relationships. Crowdfunding, online health forums and online dating help us to understand the need for stronger security measures which can increase trust judgments and minimise the risk of falling prey to fraud online.

Chapter 8, "Volunteered Surveillance," addresses the issues of data collection, data ownership, digital tracking, digital privacy, cyber security and ad-blocking in modern society through managerial, psychological and behavioural lenses. As technology advances more parties gain access to private data relying on "agree or leave" contracts, forcing individuals to give up ownership of their own behavioural patterns. These data are then commonly used for commercial purposes in forms of advertising, targeted marketing or more. Consumers on the other hand, seem to react to this in a very broad spectrum ranging from ad-blocking software to voluntary data submission. This chapter analyses why and how these reactions happen and propose solutions that could be beneficial to all parties included. This is a very novel macro concern and requires institutionalised oversight of all concerned stakeholders; governments, digital service providers and publishers, advertisers, self-regulatory organisations in related sectors and non-governmental organisations protecting consumers.

Chapter 9, "Psychological and Behavioral Examinations of Online Terrorism," presents mixed method research results on how terrorists use the internet to further their agendas. Several studies have investigated how terrorists use the online environment and the chapter first explores current knowledge about the online behaviour of terrorists. It follows on to describe how qualitative and quantitative combined studies can be used to consider how to conduct research in this area. After that a serious discussion is given to the difficult area of ethics in this field of research. The chapter closes by imparting information to the reader about the skills and knowledge necessary to undertake one's own research in this arena along with consideration of the ethics around such work.

Chapter 10, "The Role of Religiosity in Technology Acceptance: The Case of Privacy in Saudi Arabia," covers issues associated with how religion affects user behaviour and the acceptance of emerging technology. Religiosity is used to measure individual beliefs; this chapter explains how Islam influences user behaviour and intention to use technology. Saudi Arabia, as an example of a hardline Islamic nation according to the author of this chapter, is used for the discussions of privacy and technology influence in a single religion country. The chapter presents conclusions on how religion influences people's behaviour, privacy perceptions and acceptance technology.

Chapter 11, "Groups Online: Hacktivism and Social Protest," reviews the broadly defined topic of hacktivism. It offers up the proviso that it can be viewed as a legitimate form of online protest or one of illegal hacking. Additionally, there are those who feel that there is truth to both arguments, and believe it is imperative to protect those who engage in hacktivism. These counter definitions make it difficult to understand how to bridge the gap in assessing motivations. The authors give a brief introduction to hacktivism and online social protest online. In particular, the socio-psychological and cognitive factors

possibly providing the foundation for individuals to take part in hacktivism groups are addressed. Within the socio-psychological arena, the authors consider the concepts of social ties and influence. These are subfields that are important to address when looking at how individuals join, form and remain in groups. The subfield of cognitive biases is important as well and biases are examined in light of how people think and process information given the biases we each hold. Conclusions are drawn with strategies to mitigate and support vulnerabilities considering hacktivism and social protest.

Chapter 12, "A Cyber-Psychological and Behavioral Approach to Online Radicalization," addresses the challenges of bringing mainstream theories of radicalisation and cyberpsychology together with a goal towards understanding who might become radicalised. The chapter uses Islamic State of Iraq and al-Sham (ISIS) as a case study to understand how radicalised groups use cyberspace. By using academic theory, the chapter considers behavioural aspects of the radicalisation process. It also reviews how those theories are relevant in explaining, facilitating and attracting people online to a radicalisation pathway.

Chapter 13, "Insider Attack Analysis in Building Effective Cyber Security for an Organization," provides a detailed study on how behaviours from those inside may hinder security of the organisation. A number of recent studies had shown that even though there are highly advanced and secure technical controls, several cyber-attacks were carried out across multiple organisations yielding the release of confidential information. It should be clear then that technical advancements of cyber defences are not impenetrable to organisational security. Insiders often have the advantage of being a trusted party when engaging in cyber-attacks and monitoring said insiders is very challenging. The insider has the potential to cause problems to the social credibility of the organisation as well as damage its financial stability. The author reviews behaviours of insiders who may pose a cyber security threat to an organisation and provides some guidance for reliable security frameworks.

Chapter 14, "A Study of Good-Enough Security in the Context of Rural Business Process Outsourcing," presents insights using scenarios of object decomposition and sharing. By looking at low value data objects such as insurance or data-entry forms the chapter is able to explore how information is shared between a client and Rural Business Process Outsourcing (RBPO) organisations. Such sharing is usually across tasks like translation, proof-reading and data entry. These data objects are decomposed into smaller parts before being sent to the RBPO allowing for each RBPO user to only access a few parts of a complete data object. Nevertheless, this information could be leaked to unauthorised users which would breach the data security. As the value of these parts is low there is little incentive for them to truly be leaked. Here is where the idea of a good enough security system comes in. The good enough model should provide reasonable security to a group of low value data objects. This chapter describes the work of secure data assignment and leakage in RBPO. By modelling this work as an optimisation problem, the authors are able to review object decomposition scenarios in light of sharing, penalty assignment and data leakage.

Chapter 15, "Online Research Methods," opens the discussion on the use of more contemporary approaches to data collection than traditional pen and paper questionnaires. Although the traditional methods are still more readily used, various online methodologies may enhance scientific investigation and understandings of particular phenomena. The chapter explores how these could be potentially useful in understanding psychological issues related to a range of cyber security problems.

Chapter 16, "Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape," presents an overview of emerging issues in psychology of human behaviour and the evolving nature of cyber threats. The chapter reflects on the role of social engineering as the entry point of many sophisticated attacks and highlights the relevance of the human element as the starting

point of implementing cyber security programmes in organisations as well as securing individual online behaviour. Issues associated with the emerging trends in human behaviour research and ethics are presented for further discussion. The chapter concludes with a set of open research questions warranting immediate academic attention to avoid the exponential growth of information breaches in the future.

This publication addresses the emerging importance of digital psychology and the opportunities offered by cyber researchers. We hope that experts from all areas of research, information systems, psychology, sociology, human resources, leadership, strategy, innovation, law, finance and others, will find this book useful in their practice.

John McAlaney
Bournemouth University, UK

Vladlena Benson
University of West London, UK

Lara A. Frumkin
Open University, UK

Acknowledgment

First and foremost, we would like to thank our families for their patience and unresolved support during numerous late nights and weekends spent working on this book. It was a long and difficult journey for them. We would like to express our gratitude to Professors Jonathan Loo and Shanyu Tang for their valuable insights when steering this project through its final (and lengthy) stages. We would like to thank Professors Tom Buchanan and Debi Ashenden for deeming the subject of the book interesting and the project worthwhile.

We wish to thank many people who saw us through this book; to all those who provided support, talked things over, read, wrote, offered comments, and assisted in the editing, proofreading and design.

We would like to thank the IGI project team for enabling us to publish this book.

Detailed Table of Contents

Foreword xv

Preface xvii

Acknowledgment xxiv

Chapter 1
Online Decision Making: Online Influence and Implications for Cyber Security 1
Helen Joanne Wall, Edge Hill University, UK
Linda K. Kaye, Edge Hill University, UK

The growth in computer-mediated communication has created real challenges for society; in particular, the internet has become an important resource for "convincing" or persuading a person to make a decision. From a cybersecurity perspective, online attempts to persuade someone to make a decision has implications for the radicalisation of individuals. This chapter reviews multiple definitions and theories relating to decision making to consider the applicability of these to online decision making in areas such as buying behaviour, social engineering, and radicalisation. Research investigating online decision making is outlined and the point is made that research examining online research has a different focus than research exploring online decision making. The chapter concludes with some key questions for scholars and practitioners. In particular, it is noted that online decision making cannot be explained by one single model, as none is sufficient in its own capacity to underpin all forms of online behaviour.

Chapter 2
Human Factors Leading to Online Fraud Victimisation: Literature Review and Exploring the Role of Personality Traits 26
Jildau Borwell, The National Police of the Netherlands, The Netherlands
Jurjen Jansen, Open University of the Netherlands, The Netherlands & NHL University of Applied Sciences, The Netherlands & Dutch Police Academy, The Netherlands
Wouter Stol, Open University of the Netherlands, The Netherlands & NHL University of Applied Sciences, The Netherlands & Dutch Police Academy, The Netherlands

With the advent of the internet, criminals gained new tools to commit crimes. Crimes in which the use of connected information technologies is essential for the realisation of the offence are defined as cybercrimes. The human factor is often identified as the weakest link in the information security chain, and it is often the behaviour of humans that leads to the success of cybercrimes. In this chapter, end-user characteristics are studied that may predict cybercrime victimisation. This is done by means of a

review of the literature and by a study on personality traits. More specifically, personality traits from the big five are tested on victims of three different types of online fraud, phishing, Microsoft fraud, and purchasing fraud, and are compared with norm groups of the Dutch population. This chapter ends with implications for online fraud prevention and possibilities to advance the study of cyber victimisation.

Chapter 3
The "Human Factor" in Cybersecurity: Exploring the Accidental Insider 46
Lee Hadlington, De Montfort University, UK

A great deal of research has been devoted to the exploration and categorization of threats posed from malicious attacks from current employees who are disgruntled with the organisation, or are motivated by financial gain. These so-called "insider threats" pose a growing menace to information security, but given the right mechanisms, they have the potential to be detected and caught. In contrast, human factors related to aspects of poor planning, lack of attention to detail, and ignorance are linked to the rise of the accidental or unintentional insider. In this instance there is no malicious intent and no prior planning for their "attack," but their actions can be equally as damaging and disruptive to the organisation. This chapter presents an exploration of fundamental human factors that could contribute to an individual becoming an unintentional threat. Furthermore, key frameworks for designing mitigations for such threats are also presented, alongside suggestions for future research in this area.

Chapter 4
Cyber + Culture: Exploring the Relationship 64
Char Sample, US Army Research Laboratory, USA
Jennifer Cowley, US Army Research Laboratory, USA
Jonathan Z. Bakdash, U.S. Army Research Laboratory, USA

Technical advances in cyber-attack attribution continues to show incremental improvement. A growing interest in the role of the human in perception management, and decision-making suggest that other aspects of human cognition may be able to help inform attribution, and other aspects of cyber security such as defending and training. Values shape behaviors and cultural values set norms for groups of people. Therefore, they should be considered when modeling behaviors. The lack of studies in this area requires exploration and foundational work to learn the limits of this area of research. This chapter highlights some of the findings of some of the recent studies.

Chapter 5
Examinations of Email Fraud Susceptibility: Perspectives From Academic Research and Industry Practice 80
Helen S. Jones, University of Dundee, UK
John Towse, Lancaster University, UK

The internet provides an ever-expanding, valuable resource for entertainment, communication, and commerce. However, this comes with the simultaneous advancement and sophistication of cyber-attacks, which have serious implications on both a personal and commercial level, as well as within the criminal justice system. Psychologically, such attacks offer an intriguing, under-exploited arena for the understanding of the decision-making processes leading to online fraud victimisation. In this chapter, the authors focus on approaches taken to understand response behaviour surrounding phishing emails. The chapter outlines how approaches from industry and academic research might work together to more

effectively understand and potentially tackle the persistent threat of email fraud. In doing this, the authors address alternative methodological approaches taken to understand susceptibility, key insights drawn from each, how useful these are in working towards preventative security measures, and the usability of each approach. It is hoped that these can contribute to collaborative solutions.

Chapter 6

Introducing Psychological Concepts and Methods to Cybersecurity Students..... 98
Jacqui Taylor, Bournemouth University, UK
Helen Thackray, Bournemouth University, UK
Sarah E. Hodge, Bournemouth University, UK
John McAlaney, Bournemouth University, UK

This chapter begins with a brief review of the literature that highlights what psychology research and practice can offer to cybersecurity education. The authors draw on their wide-ranging inter-disciplinary teaching experience, and in this chapter, they discuss their observations gained from teaching psychological principles and methods to undergraduate and postgraduate cybersecurity students. The authors pay special attention to the consideration of the characteristics of cybersecurity students so that psychology is taught in a way that is accessible and engaging. Finally, the authors offer some practical suggestions for academics to help them incorporate psychology into the cybersecurity curriculum.

Chapter 7

The Role of Psychology in Understanding Online Trust 109
Helen S. Jones, University of Dundee, UK
Wendy Moncur, University of Dundee, UK

Across many online contexts, internet users are required to make judgments of trustworthiness in the systems or other users that they are connecting with. But how can a user know that the interactions they engage in are legitimate? In cases where trust is manipulated, there can be severe consequences for the user both economically and psychologically. In this chapter, the authors outline key psychological literature to date that has addressed the question of how trust develops in online environments. Specifically, three use cases in which trust relationships emerge are discussed: crowdfunding, online health forums, and online dating. By including examples of different types of online interaction, the authors aim to demonstrate the need for advanced security measures that ensure valid trust judgments and minimise the risk of fraud victimisation.

Chapter 8

Volunteered Surveillance 133
Subhi Can Sarıgöllü, Istanbul Bilgi University, Turkey
Erdem Aksakal, Istanbul Bilgi University, Turkey
Mine Galip Koca, Istanbul Bilgi University, Turkey
Ece Akten, Istanbul Bilgi University, Turkey
Yonca Aslanbay, Istanbul Bilgi University, Turkey

As the front end of the digitized commercial world, corporations, marketers, and advertisers are under the spotlight for taking advantage of some part of the big data provided by consumers via their digital presence and digital advertising. Now, collectors and users of that data have escalated the level of their asymmetric power with scope and depth of the instant and historical data on consumers. Since consumers

have lost the ownership (control) over their own data, their reaction ranges from complete opposition to voluntary submission. This chapter investigates psychological and societal reasons for this variety in consumer behavior and proposes that a contractual solution could promote a beneficial end to all parties through transparency and mutual power.

Chapter 9
Psychological and Behavioral Examinations of Online Terrorism 151
Sheryl Prentice, Lancaster University, UK
Paul J. Taylor, Lancaster University, UK

It has long been recognised that terrorists make use of the internet as one of many means through which to further their cause. This use of the internet has fuelled a large number of studies seeking to understand terrorists' use of online environments. This chapter provides an overview of current understandings of online terrorist behavior, coupled with an outline of the qualitative and quantitative approaches that can and have been adopted to research this phenomenon. The chapter closes with a discussion of the contentious issue of ethics in online terrorism research. The aim of the chapter is to equip readers with the necessary knowledge and skills to conduct their own research into terrorists' online behavior, taking best ethical practices into consideration when doing so.

Chapter 10
The Role of Religiosity in Technology Acceptance: The Case of Privacy in Saudi Arabia 172
Rami Mohammed Baazeem, Jeddah University, Saudi Arabia

Religion plays a major role in shaping individual behaviour, especially in the religious countries. This chapter sheds light on the effect of religiosity on the intention to use technology and privacy and will use Saudi Arabia as an example. Using the unified theory of acceptance and use of technology (UTAUT) will help explain the intention to use technology. Thus, it clarifies that the intention to use technology is affected by the user behaviour. The user's behaviour is shaped by their religious beliefs which also affect their privacy views. A systematic review of the privacy literature shows that there is a lack of study on the effect of the religious beliefs on privacy. After reading this chapter, policy makers and managers will understand that religious belief should be considered when making new laws and regulations.

Chapter 11
Groups Online: Hacktivism and Social Protest 194
Helen Thackray, Bournemouth University, UK
John McAlaney, Bournemouth University, UK

This chapter provides a brief introduction to hacktivism and social protest online and highlights some of the socio-psychological and cognitive factors that can lead to individuals taking part in hacktivism groups. Hacktivism is an ill-defined area which some claim as a legitimate form of protest in the online world and others regard as illegal hacking; there is truth to both arguments, and those who believe it should be protected will continue to work for it to be recognised. The chapter explains how the depth of social ties and influence are still being examined, and whilst cognitive biases are recognised, strategies to mitigate and combat the vulnerability they present are still being developed.

Chapter 12
A Cyber-Psychological and Behavioral Approach to Online Radicalization 210
Reyhan Topal, Bilkent University, Turkey

This chapter attempts to synthesize the mainstream theories of radicalization and the cyber-psychological and behavioral approaches with a view to identifying individuals' radicalization online. Based on the intersections of those two fields, this chapter first elaborates how radical groups use cyberspace with a specific concentration on the so-called cyber caliphate claimed by the Islamic State of Iraq and al-Sham (ISIS). Second, it revisits mainstream theories of radicalization and specifies the psychological and behavioral facets of the radicalization processes proposed by those theories. Following that, it integrates theories of radicalization with cyber-psychological and behavioral explanations of online radicalization to reveal how ISIS's use of cyberspace attracts individuals and facilitates online radicalization.

Chapter 13
Insider Attack Analysis in Building Effective Cyber Security for an Organization 222
Sunita Vikrant Dhavale, Defence Institute of Advanced Technology, India

Recent studies have shown that, despite being equipped with highly secure technical controls, a broad range of cyber security attacks were carried out successfully on many organizations to reveal confidential information. This shows that the technical advancements of cyber defence controls do not always guarantee organizational security. According to a recent survey carried out by IBM, 55% of these cyber-attacks involved insider threat. Controlling an insider who already has access to the company's highly protected data is a very challenging task. Insider attacks have great potential to severely damage the organization's finances as well as their social credibility. Hence, there is a need for reliable security frameworks that ensure confidentiality, integrity, authenticity, and availability of organizational information assets by including the comprehensive study of employee behaviour. This chapter provides a detailed study of insider behaviours that may hinder organization security. The chapter also analyzes the existing physical, technical, and administrative controls, their objectives, their limitations, insider behaviour analysis, and future challenges in handling insider threats.

Chapter 14
A Study of Good-Enough Security in the Context of Rural Business Process Outsourcing 239
Reena Singh, Manipal Institute of Technology, India
Hemant Jalota, DeepR Analytics, Canada

Data objects having low value like insurance or data-entry forms are shared between a client and rural business process outsourcing (RBPO) organisations for tasks like translation, proofreading, and data entry. These data objects are first decomposed into smaller parts and then assigned to RBPO users. Each user in a RBPO has access to only a few parts of a complete data object which he can leak to unauthorised users. But since the value of these parts is low, there is not enough incentive for the user to leak them. Such scenarios need good-enough security models that can provide reasonable security to an aggregate number of parts of low value data objects. In this chapter, the authors study the secure data assignment and leakage in RBPO by modeling it in the form of an optimisation problem. They discuss different scenarios of object decomposition and sharing, penalty assignment, and data leakage in the context of RBPO. They use LINGO toolbox to run their model and present insights.

Chapter 15
Online Research Methods 253
Linda K. Kaye, Edge Hill University, UK

With the advancement of technology and internet connectivity, the potential for alternative methods of research is vast. Whilst pen-and-paper questionnaires and laboratory studies still prevail within most scientific disciplines, many researchers are selecting more contemporary methods for undertaking research. This chapter provides an overview of a number of key online research methodologies to highlight their role in scientific investigation. In particular, it suggests how these may function to enhance our understanding of psychological issues, particularly within areas relating to cybersecurity.

Chapter 16
Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape 266
Vladlena Benson, University of West London, UK
John McAlaney, Bournemouth University, UK
Lara A. Frumkin, Open University, UK

The chapter presents an overview of emerging issues in the psychology of human behaviour and the evolving nature of cyber threats. It reflects on the role of social engineering as the entry point of many sophisticated attacks and highlights the relevance of the human element as the starting point of implementing cyber security programmes in organisations as well as securing individual online behaviour. Issues associated with the emerging trends in human behaviour research and ethics are presented for further discussion. The chapter concludes with a set of open research questions warranting immediate academic attention to avoid the exponential growth of information breaches in the future.

Compilation of References 272

About the Contributors 327

Index 332

Chapter 6
Introducing Psychological Concepts and Methods to Cybersecurity Students

Jacqui Taylor
Bournemouth University, UK

Helen Thackray
Bournemouth University, UK

Sarah E. Hodge
Bournemouth University, UK

John McAlaney
Bournemouth University, UK

ABSTRACT

This chapter begins with a brief review of the literature that highlights what psychology research and practice can offer to cybersecurity education. The authors draw on their wide-ranging inter-disciplinary teaching experience, and in this chapter, they discuss their observations gained from teaching psychological principles and methods to undergraduate and postgraduate cybersecurity students. The authors pay special attention to the consideration of the characteristics of cybersecurity students so that psychology is taught in a way that is accessible and engaging. Finally, the authors offer some practical suggestions for academics to help them incorporate psychology into the cybersecurity curriculum.

WHAT CAN PSYCHOLOGY OFFER TO CYBERSECURITY EDUCATION AND TRAINING?

There is a symbiotic relationship between the disciplines of computing and psychology: psychologists have helped in many ways to understand the way that computer systems are developed and used, but also an understanding of computers has helped psychologists to model and investigate human cognitive and social processes. This chapter will focus on the former; over the past 60 years, psychologists have

DOI: 10.4018/978-1-5225-4053-3.ch006

tracked and researched the development and impact of computers and they have also been instrumental in their design and evolution. To design, develop, implement and evaluate secure sociotechnical systems students need to understand concepts and research methods in psychology. To understand the potential risks of sociotechnical systems, cybersecurity students need to understand and consider how people perceive, remember, feel, think and solve problems, i.e. the domain of cognitive psychology. It is also important for students to consider individual differences and social behavior if effective interaction between people and computer systems is to be achieved, i.e. the domain of social psychology and individual differences. An understanding of these psychological topics enables students in cybersecurity to consider the potential capabilities and limitations of computer users and helps them to design computer systems that are more effective (usable) for a variety of user types. In addition to covering the foundation areas of Psychology, it is also important that cybersecurity students are taught evaluation methods and that they are able to consider the social impacts and ethical issues regarding the implementation and use of computer systems in organisations and society.

A review of the literature and media commentary on cybersecurity attacks shows that increasingly they involve social engineering techniques; where psychological principles are used to manipulate people into disclosing sensitive information or allowing others to access a secure system (Tetri & Vuorinen, 2013). For example, phishing emails and phone scams utilize many psychological principles relating to social influence to persuade users to open a link, such as appeals based on fear or invoking a sense of scarcity or urgency (Cialdini, 2008). However, despite the psychological nature of such cybersecurity attacks, research into the role of psychology in cybersecurity is still limited (McAlaney, Thackray and Taylor, 2016). Also, often research into the closely linked area of social engineering is conducted from the discipline of computing rather than psychology. Indeed, the call for papers for a recent conference organized in the UK by the Higher Education Academy on learning and teaching in cybersecurity listed relevant disciplines as 'STEM' and 'Computing' and the eventual program of abstracts contained no mention of psychology. Similarly, curricular guidance for the field of cybersecurity education produced by the ACM (McGettrick, 2013), contained just two uses of the word psychology and no further detail. However, within the last year the importance of psychology has begun to be recognized in the academic literature (McAlaney, Thackray and Taylor, 2016). For example, a recent article (Hamman, Hopkinson, Markham, Chaplik & Metzler, 2017) suggests the teaching of game theory in cybersecurity courses and links this to the psychological nature of many incidents. Hamman et al. propose that one of the benefits of game theory is that it fundamentally alters the way students view the practice of cybersecurity, and state that it helps to sensitize them to the human adversary element inherent in cybersecurity in addition to technology-focused best practices (p1).

The majority of psychological research that has been conducted so far in this area has focused on prevention and mitigation strategies for the targets of cybersecurity incidents with little focus on the motivation of the perpetrators (Rogers, 2010). Psychology can offer much in helping to understand the motivations of individual hackers or scammers, for example drawing on the research into individual differences, looking at factors such as self-esteem, introversion, openness to experience and social anxiety (Fullwood, 2015). Other work has shown that individual's motivations are not always related to financial gain but can be purely for entertainment or social status reasons (Rogers, 2010). In contrast, large scale cybersecurity incidents are often instigated by groups, as opposed to individuals acting alone. As such these incidents can be regarded as the result of group actions and group processes; theories from Psychology are used to help understand the formation, operation and influence of groups on their

members, and these can be usefully applied to online groups (McAlaney, Thackray and Taylor, 2016). Many hacking incidents, especially those perpetrated by teenagers and young adults, have been strongly related to social group pressure and social psychological influences. For example, individuals involved in the 2015 TalkTalk and 2011 Paypal hacks were instructed on how to do this by members of Anonymous, the hacktivist collective.

Psychological theories relating to disinhibition and deindividuation have been used to explain a number of behaviors online and can also be used to understand cybersecurity incidents. The perception of anonymity afforded by online communications allows individuals to take actions that would otherwise result in legal or social sanctions. Disinhibition refers to the sense that actions conducted online do not feel as real as those conducted offline which, it has been argued, can lead individuals to lose self-control (Taylor & MacDonald, 2002). Deindividuation, in which individuals lose their sense of self-awareness when they interact within a group, has been applied to online groups where individuals are often less identifiable and separated by space and time (Taylor & MacDonald, 2002). This is an under-researched area, but it would seem that in line with Social Identity Theory some individuals become engaged with online groups to an extent which would seem to be particularly intense and where they lose some sense of personal identity to social identity. In summary, theories from psychology can be helpful to understand and help to predict online behavior.

OBSERVATIONS FROM TEACHING PSYCHOLOGY TO CYBERSECURITY STUDENTS

In this section, the authors will review their experiences teaching psychological principles to a wide variety of cybersecurity students. The authors have experience teaching at undergraduate and postgraduate level (full-time and part-time) and developing cybersecurity training tools for industry. Foundation areas in Psychology which the authors consider important to introduce to students prior to discussing their application in cybersecurity are: social processes (e.g. group-working and communication); cognitive processes (e.g. perception, attention and memory), and individual differences (e.g. life experiences, gender, personality, cognitive style). Once these areas of psychology are covered, then it is easier to show how the authors apply psychological principles to cybersecurity.

Social Psychology and Cognition

The work of social psychologists can help understand the ways that technology affects social interaction, attitudes and behaviour. The authors ensure that there is a strong focus on how students can make practical use of the research findings and cover the major topics within Social Psychology (conversation and communication; group processes; interpersonal perception and attraction; social influence; attitudes, and conflict) and Cognitive Psychology (perception, attention and memory). Then the authors apply this understanding of social cognition to cybersecurity contexts and example topics covered include:

1. How an analysis of online language and communication can be used to identify fraudulent communication and how persuasive language can influence faulty decision-making regarding judgments of trust;

2. Group dynamics in cybersecurity incidents are reviewed, for example the group processes that shape the actions of both the cyber attackers and their intended target, including how group dynamics may lead to risky decisions and overestimations of skill and ability;
3. The psychological basis of social engineering techniques, and how these may be mitigated and prevented;
4. The role of emotion when users engage with sociotechnical systems, e.g. Frustration experienced with the technical components of a secure system have been linked to poor decision making and subsequent risky behaviour;
5. The link between cognitive load and poor online decision making;
6. New technology and organisational change is highlighted, covering issues such as the management of staff working remotely online and selection and technology enhanced training of cybersecurity personnel; and
7. The psychological elements of computer games are covered, in terms of the way gamification is used to motivate and persuade potential victims of a scam and also the authors highlight elements of addiction that may lead to poor decision-making.

Assessment and practical activities are varied and three examples are included here. The ways that online groups can influence the way their members interact and behave is addressed by asking students to devise their own scam website which aims to adopt new members to a fictitious online community. Students design experimental materials to study the links between working memory and online search strategies. Thirdly, students use and evaluate an online training package to highlight cognitive biases in cybersecurity.

Individual Differences

To illustrate individual differences in susceptibility to scams, the authors cover the following topics:

1. A psychological understanding of the cognitive deterioration in older adults and how this knowledge can be used to understand how, when and why older adults are vulnerable to financial scams;
2. How gender and personality can affect levels of online susceptibility in relation to internet dating scams;
3. How stress and cognitive style can influence poor decision making; and
4. Research from consumer psychology related to e-commerce, e.g. Individual consumer behaviour and trust in e-commerce exchanges and relations between company and consumer.

In seminars, cybersecurity undergraduates engaged well in tasks where they were asked to think from both the defence and attack perspectives. One seminar involved asking students to identify the most at-risk groups and then tailor the advice they would give to that specific group. For example, if they are advising an older adult who is unfamiliar with technology, they must think of how to explain this using simple terminology. If explaining to a child how to stay safe online, they need to use examples that children can identify with. Students were also asked to design a cyberattack that would circumnavigate their advice. The most successful exercises were highly interactive; recapping information from the most recent lecture, discussing in groups and then presenting their viewpoints to the class as a whole. It was

interesting to see that despite beginning the module with a somewhat cynical attitude to the importance of psychology, after a few seminars there was an increase in interest and participation. One large consensus from the students was that there needs to be greater emphasis on education about cybersecurity at all ages and levels of experience.

Research Methods

Cybersecurity students may have limited understanding regarding the way empirical methods (an integral part of all Psychology degrees) can be used to evaluate computer systems. To address this, topics such as Experimental Design and Internet-Mediated Research are covered. Ideally students need to experience or apply methods, therefore it is helpful if the teaching experience includes case studies and practical workshops and assessed scientific reports. The authors have run workshops which compare qualitative methods (e.g. observation, focus groups) and quantitative methods (e.g. questionnaires and performance scores) to evaluate the individual's perceived vulnerabilities and this has contrasted the different methodological approaches well.

Designing an Internet-based experiment or survey requires careful consideration. Although cybersecurity students clearly have the technical skills to conduct online surveys, they often have less understanding of experimental design and what can be done with the data. There are many benefits of Internet-mediated research (for example, access to a larger population), however, many psychological and methodological issues need to be addressed by cybersecurity students and researchers. Issues the authors cover include:

1. The difficulty in ensuring that the participant is who they say they are and that they are answering in an honest way;
2. How to gain a representative sample;
3. How to construct questionnaire items to avoid bias;
4. Issues of data screening and sample attrition rates need to be considered;
5. The demographic profiles and questionnaire scores of those who did and did not take part in online experiments or surveys need consideration, and finally
6. Ethical issues, e.g. Whether informed consent can be gained online and how debriefing will take place.

Ethics

The teaching of ethics to cybersecurity students is not new. For some time, the teaching of ethics has been a requirement on degrees accredited by the British Computer Society (BCS). Since the classic text on computer ethics (Johnson, 1985), coverage of ethics has increased as computer systems become more pervasive in daily life. For example, issues of information security such as privacy, ownership, access and liability and reliability have become more important. These advances have led to the most recent edition of computer ethics (Johnson, 2009) including much work drawing on Psychology, e.g. covering the psychological and social implications of Internet use. However, despite the increasing need for ethics teaching sometimes there can be pressure on Computing departments in meeting this requirement. This is mainly due to it being a difficult area for computing staff to teach which, according to Dark & Winstead (2005), is because the area of ethics is not positivistic in nature. As psychologists the authors

have been able to offer a different perspective on teaching ethics to cybersecurity students, based on the work of Dark & Winstead (2005), who discuss the use of educational theory and moral psychology to inform the teaching of ethics in computing-related fields. In their paper, they discuss ideas on moral development and the nature of morality, specifically as it relates to changes that educators may be trying to elicit within computing students when teaching ethics. The ways that a computer scientist and a psychologist teach ethics can be quite different, with the former more likely to use a positivist approach and the latter an approach based on educational theories. For example, a positivist approach would define what is right and what is not right (i.e. define truth) and then address what happens if one does not do what is right or does what is wrong. However, many Psychologists would disagree, saying that you cannot teach right and wrong and that although there are many laws which computing students need to know about, regarding what is wrong/right in society, there are not many things that are ethically questionable that are not illegal (and possibly vice versa!). In summary, philosophers have long recognized that it is almost impossible to 'teach' a student ethics, rather teachers need to advance students' sense of moral development and reasoning (Kohlberg & Kramer, 1969), something covered on all Psychology degrees. With this in mind, it is also important to consider the age and experience of students when designing teaching materials on ethics (covered further later). In summary, Psychologists have a lot to offer in the teaching of ethics to cybersecurity students. Some academics (Greene & Hiadt, 2002) go as far as discussing ethics purely in psychological terms, regarding the cognitive, affective and social aspects, when they state that the origins of human morality are emotions linked to expanding cognitive abilities that make people care about the welfare of others, about cooperation, cheating and norm following.

Considering the importance of individual's own behaviour around security and their understanding of the implications and consequences of behaviour, the behavioural component of morality could be of great value to teaching psychological principles to cybersecurity students; especially as learning has been shown to be aided by doing (Reese, 2011). Utilising educational games such as the Cyber Security Challenge UK has been of great value; such games set challenges for students to complete such as finding hidden data within a spread sheet. Additionally, the authors draw on students' life experiences to aid learning of the psychological materials; discussed further in the next section.

CONSIDERATION OF THE PROFILE OF CYBERSECURITY STUDENTS IN DEVELOPING PSYCHOLOGY MATERIALS

The variation between students studying different disciplines has been well documented regarding life experiences, gender and approaches to studying (Richardson, 1994). It is proposed that some of the following factors may affect the way that psychology teaching materials are perceived and understood by cybersecurity students and their level of engagement with the materials. Without wishing to generalize and stereotype students, these factors were considered in the way that materials were designed and presented with the over-arching aim to produce materials that considered and embraced individual differences.

Gender

The composition of most Psychology and Computing degree courses are significantly skewed, with females making up the majority of psychology degrees (79%) and males making up the majority (82%)

of computing degrees (Higher Education Statistical Agency, 2014). There have been many attempts to explain the reasons why males and females are attracted to different disciplines and a review of these studies shows very little support for cognitive abilities being the differentiating factor; for example, similar abilities have been found when comparing students studying social with physical sciences (Halpern, 1992). Recent research has looked at personal values, interests or motivation factors to investigate what Radford and Holdstock (1995) term, 'what people want to do rather than what they can do'. Wilson (2003) used quantitative and qualitative methods to further understanding of how Computing is perceived. In her paper she argues from a constructionist approach that, rather than any real difference in skill, female and male differences are a product of historical and cultural construction of technology as masculine (p. 128). For example, she notes that girls at school have been shown to be superior to boys in some areas of programming, but that they lack encouragement and interest so that by the time they reach 18 years of age they have already opted out. Wilson (2003) identifies teaching styles which appeal to female students as those with an emphasis on relational and contextual issues and co-operative learning through teamwork and group projects. While styles preferred by males are those that emphasize the formal and abstract and independent learning. Therefore, when teaching psychology to cybersecurity students (where there are usually more male students) traditional methods used in Psychology classes such as seminar discussions have not always been the most effective method. The authors have tried to use a broad range of methods, but recognize that some are more effective with the majority male cybersecurity students.

Life Experiences

Cybersecurity postgraduate courses tend to attract a significant number of mature entrants who have frequently been employed in other careers, have many life experiences or are currently working in a related industry and studying part-time. It is important for the contextual examples to link to real security incidents and to draw on the experiences of students. While undergraduate cybersecurity courses are more likely to attract direct-entry students, therefore the examples may be more closely linked to incidents publicized in the media.

It is important to consider stage of moral development and life experience of students when presenting materials on the topic of ethics. For example, an environment needs to be created that allows students to safely reflect on and explore their moral beliefs relative to the current issues in cybersecurity. The authors found that postgraduate students are more interested in the philosophical debates regarding the psychological and legal implications of Internet use, compared to undergraduate students. Issues that students have debated include: whether deviance online is different from deviance in face-to-face contexts; whether online addiction is similar in process to other addictions and how it might impact security vulnerabilities, and how a person's face-to-face and online identity might differ.

Gibbs, Basinger and Fuller (1992) suggest undergraduates' moral development is not fully developed; they are still developing an understanding of how moral issues may relate more generally to societal functioning. This could explain differences in debates between undergraduates and postgraduates. The postgraduate students were more open to different perspectives than undergraduates and his could be due to being older, and therefore having stronger convictions formed, or life experience within the industry. Thus, this could also be informative to the types of materials used to teach psychological principles; the postgraduates may find it easier to consider the bigger picture and societal implications of cybersecurity. While undergraduates may need more support in understanding the wider societal implications.

Motivation to Study and Learning Style

The motivation of students to study a particular course will clearly affect their engagement and there may be some initial resentment of cybersecurity students toward the topic of psychology; this needs to be considered and addressed. Many students choose psychology to help develop an understanding of themselves and others and to develop 'people' skills useful later in a range of careers. In contrast, from our observations many cybersecurity students see the course as a stepping stone to gaining almost immediate employment in the security industry or as CPD to gain promotion.

Radford and Holdstock (1995) investigated differences between reasons why students chose Computing and Psychology degrees. Students were given a list of 60 items on the 'outcomes or benefits of Higher Education' to rank. These ranged from passing exams, learning to work with others, development as a person, develop problem solving skills etc. The results showed that the most important items differentiating the two fields were that computing students chose the development of problem-solving skills, logical thinking and increasing future earning power. While for psychology students, development as a person was important as was understanding other people, oneself and greater personal independence. They identified two key factors related to a student's choice of discipline: (i) personal development versus social relationships and (ii) thinking about and directly dealing with people versus things. The implications of this for teaching psychology to cyber students are twofold: (i) that cybersecurity students may be less open to thinking about people problems when considering online threats and security, and (ii) that it is important that students are aware of the way people use technology and their interactions with others can be as important as functionality.

A considerable amount of work has been published on the relationship between personality type and learning in Further and Higher Education, although there is relatively little focusing on students from specific disciplines. Layman et al (2006) collected personality types of students studying a software engineering course using the Myers-Briggs Type Indicator (MBTI). the authors considered this when adapting our psychology materials from those designed for psychology students, in terms of: groupwork and individual work; using lectures to emphasize concepts as opposed to factual data, and materials presented objectively as matters of fact with concise, concrete explanations.

It is 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. From personal observation, cybersecurity students are generally more familiar with assessments which have definitive answers, while Psychology students are more accustomed to discussing the relative merits of both sides of a debate and to provide a balanced view rather than a definitive answer. This would support the extensive work by Kolb (1981) investigating learning styles and subject discipline. 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. Students from a cybersecurity background may be more accustomed to an epistemological and ontological stance which posits that understanding of phenomena is reached though objective study and experimental methods, and there is a finite set of solutions to any problem. In contrast the sub-disciplines of Psychology range from those which take a very positivist approach to those which are based largely on ideographic knowledge and social constructionism. Whilst the psychology topics that the authors have taught cybersecurity students do tend to lean more towards those which take a positivistic approach there is in general more subjectivity and uncertainty embedded with the teaching materials than they may be accustomed too. A comment that the authors frequently receive

from cybersecurity students is that they find it strange that many areas of psychology have no single theory that is widely accepted as being the 'correct' one, and that instead there appears to be often be a multitude of, at times mutually exclusive, theories for any given psychological phenomenon.

CONCLUSION

We would like to conclude by reflecting on our experiences to offer some general tips for those about to embark on teaching psychological principles to cybersecurity students.

As with all interdisciplinary teaching, materials need to be adapted effectively to provide appropriate links to the other discipline. In the case of cybersecurity, psychology materials need to be linked to topics taught on other units within the cybersecurity course and to show an awareness of the professional context of cybersecurity. It is important to deliver the materials at the correct level, taking into account the relevant intended learning outcomes and educational stage. At the first year of an undergraduate degree, the emphasis needs to be on practical activities and workshops can be used to demonstrate how recommendations based on Psychology can be put into practice. Indeed, examples can be used to illustrate where Psychology has *not* been considered to great effect! At final year undergraduate level, the authors found that students appreciate more detail as to *how* research was conducted and they need to develop skills to allow them to consider different psychological methods to evaluate the security of online systems. At postgraduate level, students are interested in hearing about ground-breaking research where psychology is being applied to inform cybersecurity, but also they appreciate discussing the philosophical debates. It is important not to overwhelm students (at any level) with psychological content but to provide case studies and references to support the concepts being covered. Similar to being prepared regarding the curriculum and educational level of your intended learners, some understanding of the profile of your intended learners can assist in developing Psychology materials for cybersecurity students. For example, the style of presentation of Psychology activities can be adapted to better match the approaches to studying of cybersecurity students.

Finally, it is important to recognize that students will have a certain perception of what Psychology covers. It is common for some cybersecurity students to think Psychology is only concerned with treating psychological disorders or that it is an 'un-scientific' way of explaining human behavior. As a result, it is useful at the start of any contact with cybersecurity students to briefly cover what is Psychology and what is not Psychology and to differentiate between academic Psychology and 'popular' Psychology. This helps to contextualize the wider role of Psychologists in the many areas of modern life relating to computing and technology. This has been helped recently with TV programs such as 'Hunted' (2015) employing forensic psychologists and cybersecurity experts to hunt escapees.

REFERENCES

Cialdini, R. B. (2008). *Influence: science and practice* (5th ed.). Englewood Cliffs, NJ: Prentice Hall.

Dark, M., & Winstead, J. (2005). Using educational theory and moral psychology to inform the teaching of ethics in computing. In *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development* (pp. 27-31). New York: ACM Press. doi:10.1145/1107622.1107630

Fullwood, C. (2015). The role of personality in online self-presentation. In A. Attrill (Ed.), *Cyberpsychology* (pp. 9–28). Oxford, UK: Oxford University Press.

Gibbs, J. C., Basinger, K. S., & Fuller, D. (1992). *Moral maturity: Measuring the development of sociomoral reflection*. Hillsdale, NJ: Erlbaum.

Greene, J., & Hiadt, J. (2002). How (and where) does moral judgement work? *Trends in Cognitive Sciences*, *6*(12), 517–523. doi:10.1016/S1364-6613(02)02011-9 PMID:12475712

Halpern, D. F. (1992). *Sex differences in cognitive abilities* (2nd ed.). Hillsdale, NJ: Erlbaum.

Hamman, S. T., Hopkinson, K. M., Markham, R. L., Chaplik, A. M., & Metzler, G. E. (2017). Teaching game theory to improve adversarial thinking in cybersecurity students. *IEEE Transactions on Education*, *99*, 1–7.

Higher Education Statistical Agency. (2014). *Qualifications obtained by students on HE courses at HEIs in the UK by level of qualification obtained, gender and subject area, 2012 to 2013*. Accessed on 16/12/16 from https://www.hesa.ac.uk/data-and-analysis/publications/students-2012-13/introduction

Hunted. (2015). *Channel 4 programme*. Retrieved May 30, 2017, from http://www.channel4.com/programmes/hunted

Johnson, D. (1985). *Computer ethics* (1st ed.). Englewood Cliffs, NJ: Prentice Hall.

Johnson, D. (2009). *Computer ethics* (4th ed.). Englewood Cliffs, NJ: Prentice Hall.

Kohlberg, L. & Kramer, R. (1969). Continuities and discontinuities in childhood and adult moral development. *Human Development*, *12*, 93-120.

Kolb, D. A. (1981). Learning styles and disciplinary differences. In A. W. Chickering (Ed.), *The Modern American College*. San Francisco, CA: Jossey-Bass.

Layman, L., Cornwell, T., & Williams, L. (2006). Personality types, learning styles, and an agile approach to software engineering education. *ACM SIGCSE Bulletin*, *38*(1), 428–432. doi:10.1145/1124706.1121474

McAlaney, J., Thackray, H., & Taylor, J. (2016). The social psychology of cybersecurity. *The Psychologist*, *29*(9), 686–689.

McGettrick, A. (2013). *Toward curricular guidelines for cybersecurity*. Retrieved May 30, 2017, from https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

Radford, J., & Holdstock, L. (1995). Gender differences in Higher Education aims between computing and psychology students. *Research in Science & Technological Education*, *13*(2), 163–176. doi:10.1080/0263514950130206

Reese, H. W. (2011). The learning-by-doing principle. *Behavioral Development Bulletin*, *17*(1), 1–19. doi:10.1037/h0100597

Richardson, J. T. E. (1994). Mature students in higher education: A literature survey on approaches to studying. *Studies in Higher Education*, *19*(3), 309–325. doi:10.1080/03075079412331381900

Rogers, M. K. (2010). The psyche of cybercriminals: A psycho-social perspective. In G. Ghosh & E. Turrini (Eds.), *Cybercrimes: a multidisciplinary analysis*. Berlin: Springer-Verlag.

Taylor, J., & MacDonald, J. (2002). The effects of asynchronous computer-mediated group interaction on group processes. *Social Science Computer Review*, *20*(3), 260–274. doi:10.1177/089443930202000304

Tetri, P., & Vuorinen, J. (2013). Dissecting social engineering. *Behaviour & Information Technology*, *32*(10), 1014–1023. doi:10.1080/0144929X.2013.763860

Wilson, F. (2003). Can compute, won't compute: Women's participation in the culture of computing. *New Technology, Work and Employment*, *18*(2), 127–142. doi:10.1111/1468-005X.00115