# Chapter 62
# Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape

**Vladlena Benson**
*University of West London, UK*

**John McAlaney**
*Bournemouth University, UK*

**Lara A. Frumkin**
*Open University, UK*

## ABSTRACT

*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.*

## HUMAN ELEMENT: CYBER SECURITY STARTS HERE

Cybersecurity professionals agree that that security depends on people more than on technical controls and countermeasures. Recent reviews of the cyber security threat landscape show that no industry segment is immune to cyber-attacks and the public sector tops the list for targeted security incidents (Benson, 2017). This is largely attributed to the weaker cyber security mindset of employees. On the other hand, the financial sector year on year experiences the highest volume of cyber breaches aimed

DOI: 10.4018/978-1-5225-8897-9.ch062

at financial gain or espionage. What is common between these rather different sectors is that the attack vector by cyber criminals starts with social engineering the weakest link in their security chain. With the continuous loss of control over personal information exposed online (Benson et al., 2015) individuals present easy targets for non-technical attacks ranging from spear-fishing to whaling leading on to serious cyber victimisation.

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

To gain better insights in addressing evolving challenges of the digital world, Cybersecurity increasingly relies on advances in human behaviour research. Whilst technology may often form the core of cyber-attacks, these incidents are instigated and responded to by humans. As demonstrated in recent cybersecurity breaches, such as the WannaCry ransomware affecting 150 countries, cybersecurity incidents exploit the human element. Cyber threats are increasingly choosing psychological manipulation, known as social engineering, rather than hacking in the traditional technical sense. To effectively integrate technology with the human element, a number of fields can be looked to for guidance. The military and intelligence community have been dealing with this for some time; banking and financial industries as well. Both use aspects of psychology and the human element to better detect fissures in security. If we were to ignore basic psychological research would be doing a disservice to the cybersecurity field. Understanding decision making, vigilance, and sheer convenience which undoubtedly play a role in security are essential features to understanding how to keep ourselves safe in an increasingly cyber world. Making sure that the way that employees think about keeping company data secure should match habit and personality style. Requiring frequent password changes may not be an effective strategy as people are less likely to do that then come up with a single intricate password that they use for a year. Thinking about matching the behaviours with the person is an effective strategy, we look into aligning theory to existing experiences in order to answer the following questions:

1. Can psychological manipulation of a cyber victim be countered by technical controls? – current threats mitigation measures try to establish 'expected' user profiles and identify unusual behaviours.
2. Can lapses in decision making have a measured impact on organisational and individual vigilance? – establishing metrics around appropriate decision making can help reflect preparedness of organisations towards cyber-attacks, including those manipulating employees.
3. Will cultural differences and beliefs eventually lead to idiosyncratic cyber security mechanisms? – cyber security solutions, including authentication and detection mechanisms, follow a one-size-fit-all paradigm leading to varied effectiveness.