Chapter 18
The Impact of Human Behavior on Cyber Security

Nancy Houston
Houston Educational Services, University of Advancing Technology, USA

ABSTRACT

Perhaps the greatest challenge to cyber security is that people are inherently behind each cyber problem as well as its solution. The reality is that people have been stealing secrets and information and attacking others for thousands of years; the technology of the Internet just allows it to happen at a faster pace and on a larger scale. This chapter describes aspects of human behavior that impact cyber security efforts. Cognitive overload, bias, incentives and behavioral traits all affect the decision making of both those who develop policy and strategy, those who fall victim to cyber attacks, and those who initiate cyber attacks. Although limited research has been completed on the behavioral aspects of cyber security, many behavioral principles and models are applicable to cyber security issues.

INTRODUCTION

Our way of life – from how we communicate to how business is conducted to how conflicts emerge and evolve – fundamentally depends on the Internet. Today the number of websites is approaching a billion; a rapid increase since the establishment of the first website in 1991. Cisco estimates that by 2020 there will be over 50 billion Internet-connected devices (Evans, 2011).

There is only one cyberspace, shared by military and civilian users, and everything is interconnected. "Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace" (*Cybersecurity Overview*, 2015). NATO's Jamie Shea predicts that the number of Internet users (currently 2.3 billion globally) is going to double in the next fifteen years as more and more countries in the developing world come online (Nickel, 2014). Shea says that building security into the Internet "in a way that improves public trust and confidence" is going to be one of the most important challenges of the 21st century.

Our increasing dependency on the Internet carries increased risks and often rapid and unexpected consequences – every second nine new pieces of malware are discovered. The Internet is increasingly used as a means for distributing propaganda and for inciting people to rally to a cause or take some type of action (Singer, 2014).

DOI: 10.4018/978-1-4666-8793-6.ch018

The Internet, and the hardware and software on which it depends, is both the most complex technological system ever constructed, and the most vulnerable. Network infrastructure designed to be transparent and efficient is now assaulted using techniques of such complexity that even one misplaced line or punctuation mark buried in millions of lines of code may bring about a serious breach (Husick, 2014). The Internet is never going to be perfectly secure. There are just too many moving parts and the complexity is beyond the comprehension of any team of experts.

Cybersecurity is particularly difficult because it does not follow patterns or fall in clear boxes and still lacks clear, well-accepted standard definitions. It is international, cuts across both organizational and state boundaries, and is far beyond any existing legislation. The technological volatility further complicates development of solutions that may not work in the future as they work today. The definition of cybersecurity used in this chapter is: "measures taken to protect a computer or computer system (as on the Internet) against the unauthorized access or attack" (Merriam-Webster, 2014).

BACKGROUND

The most difficult piece is perhaps that people are inherently behind each cybersecurity problem as well as its solution. People have been attacking others and stealing secrets for thousands of years. And that behavior will continue to be with us for the new digital age. Of concern is that the average level of awareness and security competence of the user base declines as the user population increases (Paganini, 2012).

Cryptographer Bruce Schneier's statements that: "Only amateurs attack machines; professionals target people. And the professionals are getting better and better." (Schneier, 2013) seem to be confirmed by research findings that 75% of network intrusions exploit weak or stolen credentials, 80% of data breaches reported by the U.S. government over a three-year period were caused by human error and device theft, and mishandled data causes 10 times more breaches than external attacks. Socially engineered cyber attacks prey on human traits such as fear, learned behavior, expectations, and greed. Even as the strength of firewalls and protective software grows, the shortest path into a network is most likely through human behavioral weakness.

Human behavior plays a major role in the effectiveness of cybersecurity efforts although the human receives far less attention than the technology. "The human operator has been treated as an abstraction within the larger human-technology system" (Tyworth, 2013). The 80-20 rule that roughly 80% of effects come from 20% of the causes applies to cybersecurity – 80% is the people and 20% is the technology (Houston, 2012).

We can be certain that the technology will continue to change as will the tools and techniques used to attack it. Yet throughout the ages, the fundamentals of human behavior have remained essentially the same. We all still take in data via our five senses. And interpretation of that data is colored by our backgrounds, experience, education and the organizational culture within which we work.

Human behavior significantly impacts how people perceive and react. Success in achieving cybersecurity depends on deep levels of human thinking and perception (situation assessment, sense making, information seeking, decision making and visualization) along with distributed collaboration (McNeese et al., 2012).

Dutt, Ahn & Gonzalez (2011) noted the difficulty of studying real-world cyber attack events because these occurrences are uncertain, and many attacks occur on proprietary networks where getting the data after the occurrence raises ownership issues. Furthermore, there are varied interests and motivations from different stakeholders who can be either attackers or defenders – business (large and small), home users, service and technology providers, government and military.