Chapter 1

The Human Factor:
Cyber Security's Greatest Challenge

George Platsis
22nd Century World, Canada

ABSTRACT

This article presents a cross spectrum of issues where the cyber domain is impacted by human decision making. Technical efforts and solutions are not enough. Therefore, until personal awareness of the cyber domain improves, we will be no closer to solving this great challenge of our time.

INTRODUCTION

The threat landscape of cyber space has changed considerably over the last 30 years. As a domain, access to it was once fairly limited, often accessible only to enterprise users, such as governments, educational institutions, and the largest corporations. But today, there are billions of users, small and large, some of which may not even realize how reliant they are on cyber space. Much the same way that many people were born into the age of electricity (and would have a difficult time imagining life without it), there is an entire generation of people that feel the same way about the Internet.

With the greater integration of technology that relies on the Internet to function into our daily lives, there will be even more access points into the cyber domain. Perhaps though, the most significant change has been our behavioral use of technology. For example, a cellular telephone, even up until the mid-2000s, was primarily used to make telephone calls, perhaps SMS text messages, and nothing else; today, a smartphone allows you to place calls, send multimedia messages, videoconference, search maps, conduct banking, monitor our health, and serve as mobile point of sale terminals, just to mention a few uses. Smartphones can even be used to hack networks.

Of course, there is a price for all these conveniences: our information. Whether it is personal or professional, our information is the newest form of currency. Yet, a paradox exists: trends show we would rather not give up our information to the Internet, but we still do so in growing fashion (Shinal, 2016). The clashes are prevalent. For example, people can claim to care about their privacy, but these same people, simultaneously, are active and prolific social media users. Corporations make efforts to employ cyber security best practices, but many do not collaborate with their supply chains or take an active

DOI: 10.4018/978-1-5225-8897-9.ch001

interest in training all levels of their staff. And governments are in a constant struggle to balance civil rights with national security interests.

In the last 30 years, perhaps the most significant changes are in the areas of size, scale, scope, and complexity of the challenges. The challenges are only magnified when 99% of computers are considered to be vulnerable (Zaharia, 2016). In other words, for every convenience comes additional vulnerability. Simultaneously, attackers are getting better and faster, moving at a rate that is outpacing the defenders' ability to protect the network and our information (Shephard, 2015).

Yet for all these challenges, the core issues are not all too different from those that professionals faced in the 1980s. To be more specific, from a historical perspective, cyber conflicts have only changed gradually, with many of the lessons of the past ignored (Healey, 2013). Perhaps this ignorance exists because we have failed to accept that most major international cyber incidents are an extension of pre-existing conflicts already in the physical domain (Gamero-Garrido, 2015).

But more importantly, the single greatest challenge in the cyber domain is also the area most often left unaddressed: the people. People do not have a uniform level of understanding of the cyber issues (Barloon, 2016), which, in turn, increases our vulnerabilities, despite our very best technical efforts. Therefore, as long as the issues related to our cyber awareness are left unaddressed – or more simply put: addressing "the people side" of the problem – we will continue to grapple with the same cyber domain challenges we are faced with today, where perhaps the only difference will be the magnitude of the problem.

This report presents a series of issues which impact a person's awareness of the cyber domain. Some of the issues are at the macro level, such as the conflict between social systems, and others are at the micro level, such as the behavior of individual users. The purpose of presenting these wide-ranging issues is to demonstrate to the reader that behind every cyber challenge, there is a person; a person who makes a decision, a person who influences a system, and a person who often stands exposed and unaware.

Despite the technical nature of the cyber domain, people will always be at its core as human error is responsible for 95% of cyber incidents (Howarth, 2014). (A discussion on the role of artificial intelligence will not be presented in this report.) Therefore, if a person does not have a sound understanding of the consequences of their actions, the ramifications could be far reaching, regardless if the end result is identity theft or a geopolitical decision that will impact multiple generations of people into the future.

THE GREATEST MACRO CHALLENGE: SYSTEMS IN OPPOSITION

Perhaps one of the reasons we are having such difficultly handling the cyber domain challenges is due to how we have traditionally defined our systems, domains, and social constructs. A brief historical analysis is useful here.

Since 1648, the Peace of Westphalia has served as the basis for the nation state. Specifically, each nation state was to have sovereignty over its territories and domestic affairs, with no interference from external powers. Respect for each other's domain was to be reciprocated. Within this system, sovereignty and enforcement of the rule of law are, more or less, universally understood and accepted. Effectively, this system created a figurative (and sometimes literal) wall to stop all others from entering one's territory.

This idea of the nation state has become the societal norm of the last 350+ years, meaning that there has generally been no disagreement as to what "a country" is. Even those with diametrically opposed worldviews on *how* to live life still accept the concept of the nation state, for the most part respecting the boundaries of the nation state, and using foreign relations as a mechanism to influence relationships.