Chapter 30
Beware!
A Multimodal Analysis of Cautionary Tales in Strategic Cybersecurity Messaging Online

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

Cautionary tales are structured stories that describe protagonists who are faced with critical decisions and often take wrong turns and suffer for it, sometimes irretrievably; these tales warn people of dangers. In cybersecurity communications, cautionary tales are an integral part of the strategic messaging. This chapter explores the uses of multimodal cautionary tales in strategic cybersecurity communications, in a convenience sampling of the following: mass-scale search terms, academic and mass media text sets, social imagery, related tags networks, and social video. This work identifies their strengths and weaknesses in suggesting methods for promoting personal cybersecurity safety. Some suggestions for higher efficacy in cybersecurity cautionary tales are suggested, in light of the advent of the Fourth Industrial Revolution.

INTRODUCTION

A basic definition of cyber reads: "relating to or characteristic of the culture of computers, information technology, and virtual reality" in Google's built-in dictionary to Google Search. For common users of cyber tools, "cyber" may evoke social spaces, distal connectivity, information-sharing, convenience for everyday life activities, entertainment, and even some bit of magic. While users may be aware of risks in cyberspace, these perils may be relegated to ephemera, the great unreal.

Whether people directly access cyberspace or not, they are vulnerable to cyber risks because of the heavy reliance on cyber for virtually every aspect of modern life (at least in the West). "Cybersecurity" refers to a wide range of efforts to try to shore up these technologies and systems to not only preserve the systems and their contents, but also their functionalities and what these provide for people's lives:

DOI: 10.4018/978-1-5225-8897-9.ch030

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access" and includes "application security, information security, network security, disaster recovery / business continuity planning, operational security (and) end-user education ("cybersecurity," Nov. 2016).

Those who are tasked with cybersecurity—in public and private sectors—have a range of tools to protect both the human populations and "cyberspace". Theirs is a mixed role because they have to maintain user confidence by not scaring users (their "installed base") unduly or else risk mass defections while encouraging proper behaviors that promote both cybersecurity and cyber safety.

Law enforcement (government) also has to make cyber a governed space, where rule-of-law applies. They have a range of tools (legal, technological, and others) to actualize this.

In the area of "end-user education," strategic messaging plays an important role. One of the strategic messaging tools that has evolved over the years is the "cautionary tale," a holdover from folklore with its oral traditions. The purpose of these stories was to warn hearers of risks, so they could avoid punishing outcomes. Most cautionary tales of old are comprised of three parts:

First, a taboo or prohibition is stated: some act, location, or thing is said to be dangerous. Then, the narrative itself is told: someone disregarded the warning and performed the forbidden act. Finally, the violator comes to an unpleasant fate, which is frequently related in expansive and grisly detail. ("Cautionary tale," May 31, 2017)

They have appeared in many forms of oral storytelling and also have been with humanity in writing as well, initially in religious texts, and then secular ones, fables, and children's stories. The core dynamic is the caution of what not to do to serve as an inoculant against poor decision-making. Cautionary tales are a popular part of pop culture; they have appeared in memes; they have appeared as exaggerated "urban legends," which could be true…but are not. Cautionary tales have even spawned "legend tripping" ("in which a cautionary tale is turned into the basis of a dare that invites the hearer to test the taboo by breaking it") ("Cautionary tale," May 31, 2017).

Some common cybersecurity taboos or prohibitions in the current age (for common users) are that thou shalt *not*…

- …share personally identifiable information (PII) in public forums
- …leak data through mishandling hardware, improperly vetting shared information, de-identifying information, or other steps
- …overshare, drunk tweet, get caught or start a tweet storm, start a feud, troll others, or misuse social media
- …take insane risks like buildering or sexting to grab attention in selfie-taking and selfie-sharing
- …respond to phishing or spear-phishing emails by giving away credentials or downloading keyloggers or malware to the local machine
- …share or download copyrighted contents online
- …install malware and spyware on a computer advertently or inadvertently
- …allow one's computers to be used as part of a botnet
- …avoid updating operating systems, software, and other dated systems
- …friend 'bots while unaware that they are 'bots