Cyber Security, Technology, and Privacy Regulation in the Digital Age

Noushin Ashrafi
University of Massachusetts Boston
Boston, MA, USA

Jean-Pierre Kuilboer
University of Massachusetts Boston
Boston, MA, USA

Christopher Schuetz
Johannes Kepler University
Linz, Austria

Abstract

In the hyper-connected world of today a breach of security is a frequent occurrence and no longer there is such thing as an isolated security threat. Breaches in one organization or system can quickly spread to others and easily get out of hand. Thus far the balance between security and privacy issues has tilted toward security. The doctrine of “nothing to hide” is one of the primary arguments made when balancing privacy against security. In the past twenty years, however, information processing has moved from the backroom to the front end, operating in a real time interactive mode. This phenomenon together with a blast of online exposure in social media and new tools available to cross-reference and mine fragmented sources has changed the information privacy landscape, where privacy, security and identity thefts have become intertwined and an ongoing cause of anxiety.

This study is based on data collected by the Identity Theft Resource Center (ITRC) and addresses a number of critical issues relating to the security challenges. We concentrate on identity thefts and analyze the trajectory of identity theft in both regulated industries such as healthcare, finance, military, and the un-regulated business sectors. As of today, except for anecdotal evidence and fragmented published data, there is little concerted examination of identity theft, which is considered the most devastating outcome of the breach of security. The public at large is aware of some of the cost/benefit tradeoffs as the Internet becomes a ubiquitous platform for social and business activities, but often underestimates the potential downsides.

Our data analysis shows no particular pattern for the number of breaches and associated records exposed over the years and across sectors. A careful look at the sectors most targeted by the threats reveals that despite sectorial security laws, self-regulatory policies, and a few technical solutions there is no evidence that the number of security breaches is declining. While compliance with information security regulations has become a top initiative in most organizations, it has not reduced the number of breaches in a noticeable way. Human factor is front and center to security breaches, whether it is by error or malicious behavior, and is considered most challenging. Understandably the majority of the attacks are targeted at electronic as compared to paper records and only a negligible percentage of paper records are exposed. Examination of sources of threats indicates that half of break-ins are known and randomly distributed between hacking of data at rest, insider break-ins, and breach of data in-transit. The other half are composed of unknown, accidental and sub-contractors, which are most challenging for organizations to monitor and control.

Despite regulatory or self-regulatory policies and security technologies, the number of security breaches is still alarmingly high. Technology advancement has created a paradox; while Privacy Enhancing Technology (PET) could and should help secure data, other technologies such as cloud computing and mobile phones are creating new threat vectors to information security as they soften the security perimeter. In terms of regulations; as information security is becoming a source of competitive advantage, compliance with regulation and legislation should be the number one initiative. A future study can also look into upcoming regulations by the US and EU and compare their impact (or lack of) on the extent and complexity of security threats.