Introduction to Information Security and Privacy in Business and Society Minitrack

Tung Bui
University of Hawaii at Manoa
tungb@hawaii.edu

Eric Clemons
University of Pennsylvania
clemons@wharton.upenn.edu

Despite the continued technological progress in cyber-security, the unauthorized disclosure of information and the intentional misuse of private information both remain pervasive worldwide – at all levels of end-user sprectum: individual, organanizational, national and global.

The purpose of this interdisciplinary minitrack is to assess the current best practices and to advance research in information security and privacy. We are interested in the attitudes of consumers or private citizens about the importance of protecting or preserving privacy, policy framework, regulations and governance. Is information security under control? What are the perspectives on risks and compliance – from the individual, corporate, and societal perspectives? Topics of interest include, but are not limited to:

- Why do security breaches continue to occur? Why can't technology be less porous and less susceptible to attack and break-in?
- Why do spear-fishing attacks and other attacks targeted at personnel and human vulnerabilities continue to succeed? Why can't employees be better trained?
- What are the impacts of current security laws, regulations and industry guidelines on privacy and security? How do laws and regulations Issues of interests would be on how laws and regulations affect information security? How do they affect corporate policy? Is compliance inadequate, or do we need better laws and regulations?
- What are the new security and privacy challenges from social networks and our emerging fully online world? How do we balance the legitimate needs of the state to protect itself and its citizens against citizens' legitimate rights to privacy? Do citizens know enough to make informed choices about the systems they use and the information that these systems disclose? Would full transparency, with clear and unambiguous corporate privacy policies result in a market in which consumers make rational and fully informed decisions? Would criminal penalties, including jail sentences, for corporate violation of stated policies, advance consumer interests? Or are regulations required, at least for minors, as they are with tobacco and alcohol?
- Are there industry-specific issues in information security and privacy? Are there fundamentally different risks in different industries, from banking, insurance, and health care, to air travel and transportation, to supply chain management in food industries or cross-border shipments?
- What are our future expectations for information security? The meaning of information security is constantly changing and expanding from a single institution to multiple organizations, and from individuals in a few industrialized nations to citizens worldwide. Should nations be legally able to develop and enforce data policies for their own nationals? Should these laws be binding on corporations domiciled elsewhere? Is the Digital Privacy Act / Right to Be Forgotten online practical? Does it address the correct issues, which may involve harmful data integration and first-degree price discrimination or outright denial of services to individuals because of prior behavior or medical conditions?
- Would the challenges triggered by information security help bring the world closer? How do the East and West diverge or converge with regards to the issues enumerated above?

We are particularly interested in research on shaping the future of information security and privacy that deals with the complex interaction among stakeholders (social actors, businesses, government agencies, etc.) in search for a symbiosis in the information age – understanding information security attitudes and behaviors; organizational culture for managing information security.