MIS QUARTERLY RESEARCH CURATION

SECURING DIGITAL ASSETS

The security of digital assets has grown from being the concern of a few technologists to an issue that impacts society at large in virtually every sector, including government, business and society. This general trend is mirrored in the pages of MIS Quarterly. Although the importance of securing digital assets was recognized as early as the journal's second year of publication (Halloran et al. 1978), research on security was relatively sparse until the last decade which has seen a marked increase of published articles on the topic. This curation highlights 57 articles published in MIS quarterly that focus on the issue of securing digital assets.

RESEARCH CURATION TEAM

Kai-Lung Hui (Hong Kong University of Science & Technology)
Anthony Vance (Virginia Tech)
Dmitry Zhdanov (Georgia State University)

PROGRESSION OF RESEARCH IN MISQ

EARLY WORK
Exploratory, focusing on uncovering new concerns and threats to digital assets.

RECENT WORK
More normative. Provide specific guidance on the design and management of information security.

CONTEXT & APPLICATIONS
System development and prototyping, cryptographic data protection, threat and risk management, end user computing, electronic data interchange and inter-organizational systems, and online exchange.

NOT ONLY WHAT, BUT HOW
Diverse methodological approaches have been applied. Demonstrates the multifaceted nature of information security, one that has engaged the behavioral, design, and economic paradigms of IS to uncover the interaction between people, technology, and policy.

.

THEMATIC ADVANCES IN KNOWLEDGE

SECUIRTY INVESTMENTS

Tangible benefits of investments in securing digital assets; Completes the "missing link"

Theoretical or normative study of information security protection will be less meaningful if the protection does not lead to tangible benefits. These articles illustrate that it does.

MARKET EFFECTS OF SECURITY ENHANCEMENT

How the nature of information security is transformed when placed inside a market; Security attacks and protection may interact beyond the organizational boundary.

Novel security externalities.

These suggest appropriate regulations and policies to address these emergent challenges.

RISK MANAGEMENT

Nature of risk management is normative.

These frame works and tools provide a convenient starting point for practitioners to strengthen organizational risk management of digital assets.

DATA BREACHES

Firm's voluntary disclosures of data breaches; Security investments and IT practices increase effectiveness of investments; Customer relationships and firm responses after breach; Learning from breaches; Individuals emotional reactions to data breach

ATTACKERS ANALYSIS

Hacker Asset Profiling; Threat prioritization; Topics in Darknet forums; Study of darknet forums, markets and attacker community

These studies believe attacks are not always random and identifying attack tools informs defenders as well. This is an early but promising area of exploration

INDIVIDUAL'S SECURITY BEHAVIOUR

Users are encouraged to adopt a protective security practice, or to avoid a harmful one.

Draws upon theories such as General Deterrence, expectancy theory, entitlement, fear appeal, protection motivation and coping

These believe people can be motivated or trained to engage in beneficial security practices and avoid harmful ones