Securing Digital Assets: An *MIS Quarterly* Research Curation

Research Curation Team:
Kai-Lung Hui *(Hong Kong University of Science and Technology)*
Anthony Vance *(Brigham Young University)*
Dmitry Zhdanov *(University of Connecticut)*

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 healthcare. 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.

1. Focus of the Research Curation

This curation highlights 32 articles published in MIS Quarterly that focus on the issue of securing digital assets (see Table 1). For scoping purposes, we do not cover closely related topics, such as disaster recovery or privacy, or include articles that feature security as a component instead of the focus of the study (e.g., "security" as a single construct of a larger model).

2. Progression of Research in MISQ

The early works on security tend to be exploratory, focusing more on uncovering new concerns and threats to digital assets. The contexts and applications vary widely, including system development and prototyping, cryptographic data protection, threat and risk management, end-user computing, electronic data interchange and inter-organizational systems, and online exchanges (Halloran et al. 1978; Murray 1979; Leitheiser and Wetherbe 1986; Post and Diltz 1986; White and Christy 1987; Hansen and Hill 1989; Loch et al. 1992; Baskerville and Stage 1996; Kumar and van Dissel 1996). For example, Boockholdt (1989) identified the emergence of new security concerns, i.e., control and backup, arising from the migration of mainframe to personal computing. Straub and Nance (1990) found that purposeful detection of security abuse were not often used, and perpetrators were not systematically disciplined. These novel findings highlight the importance of security threats to digital assets and their corresponding solutions.

By contrast, the recent published works in securing digital assets are more normative in nature. For example, Abbasi et al. (2010) developed a system to automatically detect fake websites. Johnston and Warkentin (2010) and Johnston et al. (2015) showed that fear appeals can be used to improve users' compliance with security recommendations. Vance et al. (2015) showed that user interface design can be used to increase users' accountability, and in turn, decrease noncompliant behavior. Each of these studies provide specific guidance on the actual design and management of information security.

In reviewing the progression of research on the security of digital assets in MIS Quarterly, it is interesting to observe not just what has been studied, but how. A diversity of methodological approaches have been applied, including action research (Baskerville and Stage 1996; Straub and Welke 1998; Puhakainen and Siponnen 2010; Smith et al. 2010), design science (Baskerville and Stage 1996; Abbasi et al. 2010),

economic modeling (e.g., Galbreth and Shor 2010; Chen et al. 2011; Gupta and Zhdanov 2012; Dey et al. 2014), applied econometrics (Li et al. 2012; Ransbotham et al. 2012; Kim and Kim 2014; Kwon and Johnson 2014; Wang et al. 2015), factorial survey (Vance et al. 2015), field survey (e.g., Johnston and Warkentin 2010), interpretive case study (Backhouse et al. 2006), and mixed methods (Spears and Barki 2010). These approaches demonstrate 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.

3. Thematic Advances in Knowledge

Four themes emerge from the studies listed in Table 1: (1) behavioral compliance, (2) risk management, (3) investments in securing digital assets, and (4) market effects of securing digital assets. These four themes span different units of analysis (from individual users to organizations to markets). Below, we discuss each of these research themes.

First, a major theme of research on securing digital assets appearing in MIS Quarterly is behavioral compliance, in which a user is encouraged to adopt a protective security practice, or to avoid a harmful one. Such studies have drawn on a wide range of theories from criminology and psychology, including general deterrence (Straub and Nance 1990; Harrington 1996), coping (Liang and Xue 2009), neutralization (Siponen and Vance 2010), planned behavior (Bulgurcu et al. 2010), fear appeals and protection motivation (Johnston and Warkentin 2010; Johnston et al. 2015; Boss et al. 2015; Liang and Xue 2009; Anderson and Agarwal 2010; Posey et al. 2013; Boss et al. 2015; Chen and Zahedi 2016), accountability (Vance et al. 2015), routine activity (Wang et al. 2015) and cognitive information processing and training (Puhakainen and Siponen 2010). These reference theories provide a solid foundation to holistically assess the psychological state of individuals when they appraise security threats, benefits of protection, and imposed costs of security solutions. This set of studies have affirmatively shown that the attitude and behavior towards information security is multi-dimensional. People may generally fear security threats or the consequences of misuse and noncompliance, but at the same time they may rationalize or defend poor security behavior by invoking, for example, neutralization techniques, expressive/instrumental criminal motivations, or perceptions of organizational injustice (Willison and Warkentin 2013). The consensus in these studies is that people, including home and organizational users, can be motivated or trained to engage in beneficial security practices and avoid harmful ones once we understand psychological drivers of these behaviors.

A second theme is risk management. Arguably, the nature of risk management is normative, and this is well reflected in this set of MIS Quarterly articles, which provide several practical frameworks and tools, including a probabilistic loss assessment technique based on the stochastic dominance concept in statistics (Post and Diltz 1986), a comprehensive classification of risk factors and the risk mitigation process (Baskerville and Stage 1996), a security risk planning model with security awareness education and countermeasure matrix (Straub and Welke 1998), user participation as an additional security control to enhance security awareness and alignment between IS security risk management and the business environment (Spears and Barki 2010), and the use of diversification strategies to reduce the risks of correlated failures in software deployment (Chen et al. 2011). These frameworks and tools provide a convenient starting point for practitioners to strengthen organizational risk management of digital assets.

A third theme is the investments in securing digital assets. This set of MIS Quarterly articles substantiates its tangible benefits. For example, Gordon et al. (2010) showed that voluntary disclosure of information security issues is positively associated with the market value of a firm. Li et al. (2012) found that information technology controls directly affect the quality of information produced by the system. Ransbotham et al. (2012) demonstrated that vulnerability disclosure leads to reduced vulnerability exploitation risks and attempts. Kwon and Johnson (2014) showed that security investment reduces

security failure rates, particularly when the investment is proactive. Taken together, these studies complete the "missing link" in information security research—theoretical or normative study of information security protection will be less meaningful if the protection does not lead to tangible benefits. These studies illustrate that it does.

A fourth theme is market effects of securing digital assets, which examines how the nature of information security is transformed when placed inside a market. Galbreth and Shor (2010) showed that software firms can benefit from malicious hacking because such malicious hacking nurtures a monopoly. It highlights the existence of a peculiar indirect externality due to strategic hacking. Chen et al. (2011) showed that homogeneous software design can lead to correlated failures because, by nature, the same attack can be applied to all software using the same design. There is again a peculiar negative externality due to security attacks. Gupta and Zhdanov (2012) studied the outsourcing of information security protection to managed security service providers (MSSP). It accounts for both positive and negative externalities in such outsourcing, and formally characterizes when a for-profit entity or consortium would arise. Kim and Kim (2014) showed that there is a positive "knowledge externality" in the malware resolution process. This set of MIS Quarterly articles expand our understanding of how security attacks and protection may interact beyond the organizational boundary. They also describe novel security externalities (due to strategic hacking, knowledge sharing, etc.) while also suggesting appropriate regulations and policies to address these emergent challenges.

Conclusion

This curation shows the breadth of coverage on the topic of securing digital assets, both thematically and methodologically. It also illustrates the rich phenomena and problems in this area. Finally, the contributions made by these articles provide a solid foundation for future research on the vitally important topic of securing digital assets.

Table 1. *MIS Quarterly* Papers on Securing Digital Assets.

ID	Author(s)	Title	Year	Vol.	Issue
1	J. L. Boockholdt	Implementing Security and Integrity in Micro-Mainframe Networks	1989	13	2
2	Detmar W. Straub, Jr., and William D. Nance	Discovering and Disciplining Computer Abuse in Organizations: A Field Study	1990	14	1
3	Karen D. Loch, Houston H. Carr, and Merrill E. Warkentin	Threats to Information Systems: Today's Reality, Yesterday's Understanding	1992	16	2
4	Susan J. Harrington	The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions	1996	20	3
5	Richard Baskerville and Jan Stage	Controlling Prototype Development Through Risk Analysis	1996	20	4
6	Detmar W. Straub and Richard J. Welke	Coping With Systems Risk: Security Planning Models for Management Decision Making	1998	22	4
7	James Backhouse, Carol W. Hsu, and Leiser Silva	Circuits of Power in Creating de jure Standards: Shaping an International Information Systems Security Standard	2006	30	SI
8	Huigang Liang and Yajiong Xue	Avoidance of Information Technology Threats: A Theoretical Perspective	2009	33	1

ID	Author(s)	Title	Year	Vol.	Issue
9	Ahmed Abbasi, Zhu Zhang, David Zimbra, Hsinchun Chen, Jay F. Nunamaker Jr.	Detecting Fake Websites: The Contribution of Statistical Learning Theory	2010	34	3
10	Stephen Smith, Donald Winchester, Deborah Bunker, Rodger Jaimeson	Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization	2010	34	3
11	Mikko Siponen and Anthony Vance	Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations	2010	34	3
12	Janine L. Spears and Henri Barki	User Participation in Information Systems Security Risk Management	2010	34	3
13	Burcu Bulgurcu, Hasan Cavusoglu, Izak Benbasat	Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness	2010	34	3
14	Allen C. Johnston and Merrill Warkentin	Fear Appeals and Information Security Behaviors: An Empirical Study	2010	34	3
15	Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail	Market Value of Voluntary Disclosures Concerning Information Security	2010	34	3
16	Michael R. Galbreth and Mikhael Shor	The Impact of Malicious Agents on the Enterprise Software Industry	2010	34	3
17	Catherine L. Anderson and Ritu Agarwal	Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions	2010	34	3
18	Petri Puhakainen and Mikko Siponen	Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study	2010	34	4
19	Pei-yu Chen, Gaurav Kataria, and Ramayya Krishnan	Correlated Failures, Diversification, and Information Security Risk Management	2011	35	2
20	Chan Li, Gary F. Peters, Vernon J. Richardson, and Marcia Weidenmier Watson	The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports	2012	36	1
21	Sam Ransbotham, Sabyaschi Mitra, and Jon Ramsey	Are Markets for Vulnerabilities Effective?	2012	36	1
22	Alok Gupta and Dmitry Zhdanov	Growth and Sustainability of Managed Security Services Networks: An Economic Perspective	2012	36	4
23	Robert Willison and Merrill Warkentin	Beyond Deterrence: An Expanded View of Employee Computer Abuse	2013	37	1
24	Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, Rebecca J. Bennett, and James F. Courtney	Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors	2013	37	4
25	Juhee Kwon and M. Eric Johnson	Proactive Versus Reactive Security Investments in the Healthcare Sector	2014	38	2

ID	Author(s)	Title	Year	Vol.	Issue
26	Debabrata Dey, Atanu Lahiri, and Guoying Zhang	Quality Competition and Market Segmentation in the Security Software Market	2014	38	2
27	Seung Hyun Kim and Byung Cho Kim	Differential Effects of Prior Experience on the Malware Resolution Process	2014	38	3
28	Jingguo Wang, Manish Gupta, and H. Raghav Rao	Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications	2015	39	1
29	Allen C. Johnston, Merrill Warkentin, and Mikko Siponen	An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric	2015	39	1
30	Scott R. Boss, Dennis F. Galletta, Paul Benjamin Lowry, Gregory D. Moody, and Peter Polak	What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors	2015	39	4
31	Anthony Vance, Paul Lowry, Dennis Eggett	Increasing Accountability Through User-Interface Design Artifacts: A New Approach To Addressing The Problem Of Access-Policy Violations	2015	39	2
32	Yan Chen and Fatemeh Mariam Zahedi	Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China	2016	40	1

Please cite this curation as follows: Hui, K.L., Vance, A., Zhdanov, D. "Securing Digital Assets," in MIS Quarterly Research Curations, Ashley Bush, ed., http://misq.org/research-curations, May 27, 2016.