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 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. This curation highlights 32 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 and Technology)*
Anthony Vance *(Temple University)*
Dmitry Zhdanov *(Georgia State University)*

Progression of Research in MISQ

Early Work

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

Contexts and applications include: system development and prototyping, cryptographic data protection, threat and risk management, end-user computing, electronic data interchange and inter-organizational systems, and online exchanges

Recent Work

More normative.

Provide specific guidance on the design and management of information security.

Not Only What But *How*

A diversity of 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

Behavioral Compliance

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

These articles have drawn on a wide range of theories.

The consensus in this group of articles is that people can be motivated or trained to engage in beneficial security practices and avoid harmful ones once we understand psychological drivers of these behaviors.

Risk Management

The nature of risk management is normative, and this is well reflected in this group of articles which provide several practical frameworks and tools.

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

Investments in Securing Digital Assets

This group of articles substantiates the tangible benefits of investments in securing digital assets.

Taken together, these articles 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 articles illustrate that it does.

Market Effects of Securing Digital Assets

Examines how the nature of information security is transformed when placed inside a market.

This set of articles expands our understanding of how security attacks and protection may interact beyond the organizational boundary. They also describe novel security externalities while also suggesting appropriate regulations and policies to address these emergent challenges.

MIS Quarterly Articles on Securing Digital Assets

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

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

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

33. Kai-Lung Hui, Seung Hyun Kim, and Qiu-Hong Wang, ***Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks***, 2017, 41, 2

34. Sigi Goode, Viswanath Venkatesh, and Susan A. Brown, ***User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach***, 2017, 41, 3

35. Corey M. Angst, Emily S. Block, John D'Arcy, and Ken Kelley, ***When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches***, 2017, 41, 3

36. Gregory D. Moody, Mikko Siponen, and Seppo Pahnila, ***Toward a Unified Model of Information Security Policy Compliance***, 2018, 42, 1