MISQ Research Curation on Securing Digital Assets

Research Curation Team:
Kai-Lung Hui (*Hong Kong University of Science and Technology*)
Anthony Vance (*Virginia Tech*)
Dmitry Zhdanov (*Illinois State University*)

Release Date: May 2016
Updated: July 2018, April 2023

The security of digital assets has grown from being the concern of a few technologists to an issue that impacts individuals and organizations in virtually every sector, including government, business, and society. This general trend is mirrored in the pages of *MIS Quarterly*. Although the importance of security was recognized as early as the journal's second year of publication (Halloran et al. 1978), research on security was sparse until a 2010 *MIS Quarterly* special issue, "Information Systems Security in the Digital Economy" (Mahmood et al. 2010), which marked the beginning of sustained interest in articles dealing with security both at *MIS Quarterly* and the IS field in general. This update of the curation reflects the growing diversity of both problems studied and methods adopted and introduces new research themes—attacker analysis and data breaches—for the first time.

1. Focus of the Research Curation

This curation highlights 57 articles published in *MIS Quarterly* that focus on security[1] (see Table 1). For scoping purpose, we do not cover closely related topics, such as disaster recovery, or privacy or trust, which have their own MISQ research curations (Popovic et al. 2019; Söllner et al. 2018). We also do not include articles that feature security as a component, rather than the focus of the study (e.g., "security" as a single construct of a larger model).

2. Progression of Research in MISQ

Early works on security tend to be exploratory, focusing more on uncovering new concerns and security threats. 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 was not often used, and perpetrators were

[1] Various terms for security have been used in *MIS Quarterly* over time, including "security" (Halloran et al. 1978), "data security" (Rittenberg and Purdy 1978), "computer security" (Cheney and Lyons 1980), "information security" (Dickson et al. 1984), "network security" (Hall and McCauley 1987), and "cybersecurity" (Anderson and Agarwal 2010). In recent years "cybersecurity" has become more common, reflecting usage in industry and popular media. In this curation, we use the term "security" broadly to encompass all of these terms.

not systematically disciplined. These novel findings highlight the importance of security threats to digital assets and their corresponding solutions.

By contrast, later published works in security 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 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 Siponen 2010; Smith et al. 2010), design science (Baskerville and Stage 1996; Abbasi et al. 2010; Samtani et al. 2022; Li and Chen forthcoming), 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; Angst et al. 2017; Hui et al. 2017), factorial survey (Vance et al. 2015, Hamid and Grover forthcoming), field survey (e.g., Johnston and Warkentin 2010; Goode et al. 2017; Hoehle et al. 2022), laboratory experiments (Boss et al. 2015; Liang et al. 2019), interpretive case study (Backhouse et al. 2006), machine learning and natural language processing (Bachura et al. 2022; Samtani et al. 2022; Li and Chen forthcoming), mixed methods (Spears and Barki 2010, Vance et al. 2022; Nikkhah and Grover forthcoming), and NeuroIS (Vance et al. 2018, Turel et al. 2021). These approaches demonstrate the multifaceted nature of 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

Six themes emerge from the studies listed in Table 1: (1) individuals' security behavior, (2) risk management, (3) investments in security, (4) market effects of security, (5) attacker analysis, and (6) data breaches. These themes span different units of analysis (from individual users to organizations to markets). Below, we discuss each of these research themes.

Individual's security behaviors

First, a major theme of research on security appearing in MIS Quarterly is individual behavior. A significant branch of this theme examines the threat to organizations, of employees committing computer abuse or violating information security policies. These studies use theories from economics, criminology, and psychology to explain violations and abuse, such as general deterrence (Straub and Nance 1990; Harrington 1996), neutralization (Siponen and Vance 2010, Willison and Warkentin 2013), accountability (Vance et al. 2015), routine activity (Wang et al. 2015), planned behavior (Bulgurcu et al. 2010), criminal opportunity (Wang et al. 2019), expectancy theory (Turel et al. 2021), and entitlement (Amo et al. 2022). Moody et al. (2018) performed a unified model that combines many key constructs from these theories. Cram et al. (2019) provide a meta-analysis of this literature, finding that attitude, personal norms and ethics, and normative beliefs had the strongest effects, whereas punishment and reward related constructs

exhibited the weakest effects.

Another branch of this theme studies how individuals can be encouraged to adopt a protective security practice (such as backing up data, Boss et al. 2015), avoid a harmful one (e.g., installing malware, Liang et al. 2019). Many of these studies use theories from the health belief literature, such as fear appeal or protection motivation theory (Johnston and Warkentin 2010; Anderson and Agarwal 2010, Posey et al. 2013, Boss et al. 2015, Chen and Zahedi 2016, Vance et al. 2022), or related theories of coping or threat avoidance (Liang and Xue 2009, Liang et al. 2019). These studies assess the psychological state of individuals when they appraise security threats, benefits of protection, and imposed costs of security solutions. Other studies use different theoretical foundations such as habituation theory from neurobiology to explain adherence to security warnings (Vance et al. 2018) and contextual theory (Wright et al. forthcoming) to explain adherence to phishing. The consensus of these studies is that individuals can be motivated or prompted to engage in beneficial security practices and avoid harmful ones once we understand psychological drivers of these behaviors.

Risk management

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.

Security investments

A third theme is investments in security enhancement. This set of *MIS Quarterly* articles substantiates its tangible benefits. For example, 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. Hui et al. (2017) showed that law enforcement deters cybercrimes particularly with international cooperation, and that there is network and displacement effects in the enforcement. Angst et al. (2017) found that investment in IT security in itself does not result in fewer data breaches, but meaningful integration of IT security with IT processes and practices does lead to fewer data breaches over time. Taken together, these studies complete the "missing link" in security research—theoretical or normative study of security protection will be less meaningful if the protection does not lead to tangible benefits. These studies illustrate that it does.

Market effects of security enhancement

A fourth theme is market effects of security enhancement, which examines how the nature of 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 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.

Attacker analysis

The 2022 revision to this curation adds a fifth theme, attacker analysis. In an editorial, Mahmood et al. (2010) called for IS researchers to study attackers' motivations and techniques. However, previous work in security generally took the defender's perspective and treated the environment as the source of stochastic threats. Yet there is a growing understanding that many attacks are not random and that identifying emergent attack tools and techniques informs defenders as well. To this end, Ebrahimi et al. (2022) designed a cross-lingual IT artifact to facilitate hacker asset profiling. Samtani et al. (2022) developed an automated threat prioritization method. Li and Chen (forthcoming) automated the emerging topic identification in darknet forums. Yue et al. (2019) analyzed whether distributed denial of service (DDoS) attack mentions in hacker forums affects DDoS attacks globally. A common feature of these works is the study of darknet forums and markets and the attacker community, usually combined with some form of text processing, machine learning, and design science approaches. This is an early but promising area of exploration for IS researchers.

Data breaches

A sixth theme, also new in the 2022 curation revision, is data breaches. Studies involving data breaches have been featured in this curation previously (e.g., Gordon et al. 2010 under the theme of security investments). However, a growing number of articles on this topic using diverse methods justified data breaches becoming a theme in its own right. Gordon et al. 2010 first examined data breaches in *MIS Quarterly* as part of firms' voluntary disclosures about security. They discovered that through voluntary disclosures of data breaches in the firm's financial reports, announcements of data breaches in combination with proactive security activities and potential vulnerabilities significantly increased firm's market value.
Other studies have examined whether security investments can predict data breaches. Kwon and Johnson (2014) showed that proactive security investments are associated with fewer rates of data breaches. They further found that proactive investments are more cost effective than reactive

investments made after a data breach occurs. Angst et al. (2017) demonstrated that more security investments do not necessarily reduce data breaches, but that substantive adoption of IT practices increases the effectiveness of security investments, whereas symbolic adoption has the opposite effect. Li et al. (forthcoming) found that security investments do not of themselves decrease the occurrence of data breaches, but that security investments combined with threat awareness, as measured by a firm's voluntary disclosure of security activities, do reduce data breaches.

Another facet of data breach research is on how to manage customer relationships after a breach. Goode et al. (2017) investigated customer compensation as a response strategy in the wake of the 2011 Sony PlayStation breach. They found that compensation can be an effective means of increasing perceptions of service quality and repurchase intentions, as long as expectations are met within a zone of tolerance. However, repurchase intentions are reduced when expectations for compensation are not met. Hoehle et al. (2022) extended this work by showing that distributive and procedural justice perceptions mediate the effect of compensation expectations on outcomes such as continued shopping intention and online complaining. They also showed that, in certain cases, compensating customers beyond what is expected can negatively influence justice perceptions. Nikkhah and Grover (forthcoming) examined company-issued letters following data breaches to identify response strategies. Through factorial survey and event studies, they showed that accommodation strategies such as apologizing, taking corrective action, and offering compensation can moderate the negative impact of data breaches on customer intentions and cumulative abnormal returns for investors. However, these accommodative strategies are themselves moderated by a company's response time, constituting a three-way interaction effect.

In contrast to the other papers in this theme that examined company strategies relating to data breaches, Mehrizi et al. (2022) examine how organizations learn from IS incidents, including data breaches. They provide a framework that integrates different learning modes that organizations use to learn from security incidents. Bachura et al. (2022) focus on individuals' emotional reactions to a data breach. Through longitudinal analysis of more than 18,000 messages on Twitter in the wake of the breach at the U.S. Office of Personnel Management in 2015, the authors describe a shared emotional experience of anxiety, anger, and sadness. This study provides a unique perspective of the emotional costs of data breaches.

Conclusion

This curation shows the breadth of coverage on the topic of security, both thematically and methodologically. It establishes that security is a mainstream area of IS research and illustrates the rich phenomena and range of problems in this area. Finally, the contributions made by these articles show the research opportunities for studying evolving threats in the vitally important topic of security.

Please cite this curation as follows: Hui, K.L., Vance, A., Zhdanov, D. "Securing Digital Assets," in *MIS Quarterly Research Curations*, Ashley Bush and Arun Rai, Eds., https://www.misqresearchcurations.org/blog/2017/5/10/trust-1, April 2023. doi: 10.25300/05272016

References

Cheney, Paul and Lyons, Norman. 1980. “Information Systems Skill Requirements: A Survey,” MIS Quarterly, 4 (1), 35–43.

Dickson, Gary; Leitheiser, Robert; and Wetherbe, James. 1984. “Key Information Systems Issues for the 1980’s,” *MIS Quarterly*, 8 (3), pp. 135–139.

Hall, Wayne and McCauley, Robert. 1987. "Planning and Managing a Corporate Network Utility," MIS Quarterly, 11 (4), pp. 437–449.

Hansen, James, Hill, Ned. 1989. “Control and Audit of Electronic Data Interchange,” *MIS Quarterly*, 13 (4), pp. 403–413.

Halloran, Dennis; Manchester, Susan; Moriarty, John; Riley, Robert; Rohrman, James; Skramstad, Thomas. 1978. “Systems Development Quality Control,” *MIS Quarterly*, 2 (1), pp. 1–13.

Kumar, Kuldeep, Van Diesel, Han. 1996. “Sustainable Collaboration: Managing Conflict and Cooperation in Interorganizational Systems,” *MIS Quarterly*, 20 (3), pp. 279–300.

Leitheiser, Robert and Wetherbe, James. 1986. “Service Support Levels: An Organized Approach to End-User Computing,” *MIS Quarterly*, 10 (4), pp. 337–349.

Mahmood, Adam M.; Siponen, Mikko; Straub, Detmar W.; Rao, Raghav; and Raghu, T S. 2010. “Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue,” MIS Quarterly, (34: 3) pp. 431–433.

Murray, Thomas. 1979. “Cryptographic Protection of Computer-Based Data Files,” *MIS Quarterly*, 3 (1), pp. 21–28.

Popovic, A., Thong, J.Y.L., and Wattal, S. 2019. “Information Privacy,” in *MIS Quarterly* Research Curations, Ashley Bush and Arun Rai, Eds., http://misq.org/research-curations, doi: 10.25300/05292017

Post, Gerard and Diltz, J. David 1986. “A Stochastic Dominance Approach to Risk Analysis of Computer Systems,” MIS Quarterly, 10 (4), pp. 363–375.

Rittenberg, Larry and Purdy, Charles. 1978. “The Internal Auditor's Role in MIS Developments,” *MIS Quarterly*, 2 (1), pp. 47–57.

Söllner, M., Benbasat, I., Gefen, D., Leimeister, J. M., Pavlou, P. A. 2018. “Trust,” in MIS Quarterly Research Curations, Ashley Bush and Arun Rai, Eds., https://www.misqresearchcurations.org/blog/2017/5/10/trust-1, doi: 10.25300/10312016

White, Clinton and Christy, David. 1987. “The Information Center Concept: A Normative Model and a Study of Six Installations,” MIS Quarterly, 11 (4), pp. 451–458.

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
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

ID	Author(s)	Title	Year	Vol.	Issue
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

ID	Author(s)	Title	Year	Vol.	Issue
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
37	Vance A., Jenkins J.L., Anderson B.B., Bjornn D.K., Kirwan C.B.	Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments	2018	42	2
38	Kwon J., Johnson M.E.	Meaningful healthcare security: Does meaningful-use attestation improve information security performance?	2018	42	4

ID	Author(s)	Title	Year	Vol.	Issue
39	Yue W.T., Wang Q.-H., Hui K.-L.	See no evil, hear no evil? Dissecting the impact of online hacker forums	2019	43	1
40	Bose I., Leung A.C.M.	Adoption of identity theft countermeasures and its short- And long-term impact on firm value	2019	43	1
41	Wang J., Shan Z., Gupta M., Raghav Rao H.	A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts	2019	43	2
42	Liang H., Xue Y., Pinsonneault A., Wu Y.	What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective	2019	43	2
43	Cram Alec W. , D'Arcy J., Proudfoot J.G.	Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance	2019	43	2
44	Yoo C.W., Goo J., Rao H.R.	Is cybersecurity A team sport? A multilevel examination of workgroup information security effectiveness	2020	44	2
45	Pallab Sanyal, Nirup M. Menon, Mikko Siponen	An Empirical Examination of the Economics of Mobile Application Security	2021	45	4
46	Ofir Turel, Un Qinghua He, Yatong Wen	Examining the Neural Basis of Information Security Policy Violations: A Noninvasive Brain Stimulation Approach	2021	45	4
47	Hartmut Hoehle, Viswanath Venkatesh, Sue Brown, Bennett J. Tepper, Thomas Kude	Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal Study of Target's Data Breach	2022	46	1
48	Mohammad Rezazade Mehrizi, Davide Nicolini, Juan Rodon Modol	How Do Organizations Learn from Information System Incidents? A Synthesis of the Past, Present, and Future	2022	46	1
49	Sagar Samtani, Yidong Chai, and Hsinchun Chen	Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model	2022	46	2
50	Eric Bachura, Rohit Valecha, Rui Chen, and H. Raghav Rao	The OPM Data Breach: An Investigation of Shared Emotional Reactions on Twitter	2022	46	2

ID	Author(s)	Title	Year	Vol.	Issue
51	Mohammadreza Ebrahimi, Yidong Chai, Sagar Samtani, and Hsinchun Chen	Cross-Lingual Cybersecurity Analytics in the International Dark Web with Adversarial Deep Representation Learning	2022	46	2
52	Laura C. Amo, Emily Grijalva, Tejaswini Herath, G. James Lemoine, and H. Raghav Rao	Technological Entitlement: It's My Technology and I'll (Ab)Use It How I Want To	2022	46	3
53	Anthony Vance, David Eargle, Dennis Eggett, Detmar Straub, Kirk Ouimet	Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examinations of Password Strength	2022	46	3
54	Wilson Weixun Li, Alvin Chung Man Leung, and Wei Thoo Yue	Where is IT in Information Security? The Interrelationship Among IT Investment, Security Awareness, and Data Breaches	2023	47	1
55	Weifeng Li and Hsinchun Chen	Discovering Emerging Threats in the Hacker Community: A Nonparametric Emerging Topic Detection Framework	2022	46	4
56	Hamid Reza Nikkhah and Varun Grover	An Empirical Investigation of Company Response to Data Breaches	2022	46	4
57	Ryan T. Wright, Steven L. Johnson, and Brent Kitchens	Phishing Susceptibility in Context: A Multi-level Information Processing Perspective on Deception Detection	Forthcoming		

Curated References:

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., and Jay F. Nunamaker, J. 2010. "Detecting Fake Websites: The Contribution of Statistical Learning Theory," *MIS Quarterly* (34:3), pp. 435–461. Also available at https://aisel.aisnet.org/misq/vol34/iss3/5/

Amo, L. C., Grijalva, E., Herath, T., Lemoine, G. J., and Rao, H. R. 2022. "Technological Entitlement: It's My Technology and I'll (Ab)Use It How I Want To," *MIS Quarterly* (46:3), pp. 1395-1420. Also available at https://aisel.aisnet.org/misq/vol46/iss3/8/

Anderson, C. L., and Agarwal, R. 2010. "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly* (34:3), pp. 613–643. Also available at https://aisel.aisnet.org/misq/vol34/iss3/13/

Angst, C. M., Block, E. S., Arcy, J. D., and Kelley, K. 2017. "When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches," *MIS Quarterly* (41:3), pp. 893–916. Also available at https://aisel.aisnet.org/misq/vol47/iss1/13/

Bachura, E., Valecha, R., Chen, R., and Rao, H. R. 2022. "The OPM Data Breach: An Investigation of Shared Emotional Reactions on Twitter," *MIS Quarterly* (46:2), pp. 881-910. Also available at https://aisel.aisnet.org/misq/vol46/iss2/10/

Backhouse, J., Hsu, C. W., and Leiser, S. 2006. "Circuits of Power in Creating de Jure Standards: Shaping an International Information Systems Security Standard," *MIS Quarterly* (30:SI), pp. 413–438. Also available at https://aisel.aisnet.org/misq/vol34/iss3/6/

Baskerville, R. L., and Stage, J. 1996. "Controlling Prototype Development Through Risk Analysis," *MIS Quarterly* (20:4), pp. 481–501. Also available at https://aisel.aisnet.org/misq/vol20/iss4/5/

Boockholdt, J. L. 1989. "Implementing Security and Integrity in Micro-Mainframe Networks," *MIS Quarterly* (13:2), pp. 135–144. Also available at https://aisel.aisnet.org/misq/vol13/iss2/2/

Bose, I., and Leung, A. C. M. 2019. "Adoption of Identity Theft Countermeasures and Its Short- And Long-Term Impact on Firm Value," *MIS Quarterly* (43:1), pp. 313–327. Also available at https://aisel.aisnet.org/misq/vol43/iss1/16/

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. "What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors," *MIS Quarterly* (39:4), pp. 837–864. Also available at https://aisel.aisnet.org/misq/vol39/iss4/7/

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523–548. Also available at https://aisel.aisnet.org/misq/vol34/iss3/9/

Chen, P., Kataria, G., and Krishnan, R. 2011. "Correlated Failures, Diversification, and Information Security Risk Management," *MIS Quarterly* (35:2), pp. 397–422. Also available at https://aisel.aisnet.org/misq/vol35/iss2/9/

Chen, Y., and Zahedi, F. M. 2016. "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China," *MIS Quarterly* (40:1), pp. 205–222. Also available at https://aisel.aisnet.org/misq/vol40/iss1/11/

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525-554. Also available at https://aisel.aisnet.org/misq/vol43/iss2/10/

Dey, D., Lahiri, A., and Zhang, G. 2014. "Quality Competition and Market Segmentation in the Security Software Market," *MIS Quarterly* (38:2), pp. 589–606. Also available at https://aisel.aisnet.org/misq/vol38/iss2/14/

Ebrahimi, M., Chai, Y., Samtani, S., and Chen, H. 2022. "Cross-Lingual Cybersecurity Analytics in the International Dark Web with Adversarial Deep Representation Learning," *MIS Quarterly* (46:2), pp. 1209-1226. Also available at https://aisel.aisnet.org/misq/vol46/iss2/21/

Galbreth, M. R., and Shor, M. 2010. "The Impact of Malicious Agents on the Enterprise Software Industry," *MIS Quarterly* (34:3), pp. 595–612. Also available at https://aisel.aisnet.org/misq/vol34/iss3/12/

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach," *MIS Quarterly* (41:3), pp. 703–727. Also available at https://aisel.aisnet.org/misq/vol41/iss3/5/

Gordon, L. A., Loeb, M. P., and Sohail, T. 2010. "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly* (34:3), pp. 567–594. Also available at https://aisel.aisnet.org/misq/vol34/iss3/11/

Gupta, A., and Zhdanov, D. 2012. "Growth and Sustainability of Managed Security Services Networks: An Economic Perspective," *MIS Quarterly* (36:4), pp. 1109–1130. Also available at https://aisel.aisnet.org/misq/vol36/iss4/13/

Harrington, S. J. 1996. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* (20:3), pp. 257–277. Also available at https://aisel.aisnet.org/misq/vol20/iss3/1/

Hoehle, H., Venkatesh, V., Brown, S. A., Tepper, B. J., and Kude, T. 2022. "Impact of Customer Compensation Strategies on Outcomes and the Mediating Role of Justice Perceptions: A Longitudinal Study of Target's Data Breach," *MIS Quarterly* (46:1), pp. 249–340. Also available at https://aisel.aisnet.org/misq/vol46/iss1/13/

Hui, K.-L., Kim, S. H., and Wang, Q.-H. 2017. "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks," *MIS Quarterly* (41:2), pp. 497–523. Also available at https://aisel.aisnet.org/misq/vol41/iss2/10/

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549–566. Also available at https://aisel.aisnet.org/misq/vol34/iss3/10/

Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113–134. Also available at https://aisel.aisnet.org/misq/vol39/iss1/8/

Kim, S. H., and Kim, B. C. 2014. "Differential Effects of Prior Experience on the Malware Resolution Process," *MIS Quarterly* (38:3), pp. 655–678. Also available at https://aisel.aisnet.org/misq/vol38/iss3/4/

Kwon, J., and Johnson, M. E. 2014. "Proactive Versus Reactive Security Investments in the Healthcare Sector," *MIS Quarterly* (38:2), pp. 451–471. Also available at https://aisel.aisnet.org/misq/vol38/iss2/8/

Kwon, J., and Johnson, M. E. 2018. "Meaningful Healthcare Security: Does 'Meaningful-Use' Attestation Improve Information Security Performance?," *MIS Quarterly* (42:4), pp. 1043–1067. Also available at https://aisel.aisnet.org/misq/vol42/iss4/4/

Li, C., Peters, G. F., Richardson, V. J., and Watson, M. W. 2012. "The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports," *MIS Quarterly* (36:1), pp. 179–203. Also available at https://aisel.aisnet.org/misq/vol36/iss1/14/

Li, W., and Chen, H. 2022. "Discovering Emerging Threats in the Hacker Community: A Nonparametric Emerging Topic Detection Framework," *MIS Quarterly* (44:4), pp. 2337–2350. Also available at https://aisel.aisnet.org/misq/vol46/iss4/22/

Li, W. W., Leung, A. C. M., and Yue, W. T. 2023. "Where Is IT in Information Security? The Interrelationship Among IT Investment, Security Awareness, and Data Breaches," *MIS Quarterly* (47:1), pp. 317–342. Also available at https://aisel.aisnet.org/misq/vol47/iss1/13/

Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly* (33:1), pp. 71–90. Also available at https://aisel.aisnet.org/misq/vol33/iss1/6/

Liang, H., Xue, Y., Pinsonneault, A., and Wu, Y. A. 2019. "What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective," *MIS Quarterly* (43:2), pp. 373-394. Also available at https://aisel.aisnet.org/misq/vol43/iss2/4/

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp. 173–186. Also available at https://aisel.aisnet.org/misq/vol16/iss2/2/

Mehrizi, M. H. R., Nicolini, D., and Mòdol, J. R. 2022. "How Do Organizations Learn from Information System Incidents? A Synthesis of the Past, Present, and Future," *MIS Quarterly* (46:1), pp. 531-590. Also available at https://aisel.aisnet.org/misq/vol46/iss1/20/

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285–311. Also available at https://aisel.aisnet.org/misq/vol42/iss1/16/

Nikkhah, H. R., and Grover, V. 2022. "An Empirical Investigation of Company Response to Data Breaches," *MIS Quarterly* (46:4), pp. 2163–2196. Also available at https://aisel.aisnet.org/misq/vol46/iss4/16/

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. "Insiders' Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors," *MIS Quarterly* (37:4), pp. 1189–1210. Also available at https://aisel.aisnet.org/misq/vol37/iss4/11/

Puhakainen, P., and Siponen, M. 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757–778. Also available at https://aisel.aisnet.org/misq/vol34/iss4/9/

Ransbotham, S., Mitra, S., and Ramsey, J. 2012. "Are Markets for Vulnerabilities Effective?," *MIS Quarterly* (36:1), pp. 43–64. Also available at https://aisel.aisnet.org/misq/vol36/iss1/6/

Samtani, S., Chai, Y., and Chen, H. 2022. "Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model," *MIS Quarterly* (46:2), pp. 911-946. Also available at https://aisel.aisnet.org/misq/vol46/iss2/11/

Sanyal, P., Menon, N., and Siponen, M. 2021. "An Empirical Examination of the Economics of Mobile Application Security," *MIS Quarterly* (45:4), pp. 2235-2260. Also available at https://aisel.aisnet.org/misq/vol45/iss4/23/

Siponen, M., and Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Systems Security Policy Violations," *MIS Quarterly* (34:3), pp. 487–502. Also available at https://aisel.aisnet.org/misq/vol34/iss3/7/

Smith, S., Winchester, D., Bunker, D., and Jamieson, R. 2010. "Circuits of Power: A Study of Mandated Compliance to an Information Systems Security De Jure Standard in a Government Organization," *MIS Quarterly* (34:3), pp. 463–486. Also available at https://aisel.aisnet.org/misq/vol34/iss3/6/

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503–522. Also available at https://aisel.aisnet.org/misq/vol34/iss3/8/

Straub, D. W., and Nance, W. D. 1990. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* (14:1), pp. 45–60. Also available at https://aisel.aisnet.org/misq/vol14/iss1/3/

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4), pp. 441–464. Also available at https://aisel.aisnet.org/misq/vol22/iss4/2/

Turel, O., He, Q., and Wen, Y. 2021. "Examining the Neural Basis of Information Security Policy Violations: A Noninvasive Brain Stimulation Approach," *MIS Quarterly* (45:4), pp. 1715-1744. Also available at https://aisel.aisnet.org/misq/vol45/iss4/7/

Vance, A., Eargle, D., Eggett, D., Straub, D., and Ouimet, K. 2022. "Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examination of Password Strength," *MIS Quarterly* (46:3), pp. 1721-1738. Also available at https://aisel.aisnet.org/misq/vol46/iss3/19/

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., and Kirwan, C. B. 2018. "Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through FMRI, Eye Tracking, and Field Experiments," *MIS Quarterly* (42:2), pp. 355-380. Also available at https://aisel.aisnet.org/misq/vol42/iss2/3/

Vance, A., Lowry, P. B., and Eggett, D. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing The Problem Of Access-Policy Violations," *MIS Quarterly* (39:2), pp. 345–366. Also available at https://aisel.aisnet.org/misq/vol39/iss2/6/

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly* (39:1), pp. 91–112. Also available at https://aisel.aisnet.org/misq/vol39/iss1/7/

Wang, J., Shan, Z., Gupta, M., and Rao, H. R. 2019. "A Longitudinal Study of Unauthorized Access Attempts on Information Systems: The Role of Opportunity Contexts," *MIS Quarterly* (43:2), pp. 601-622. Also available at https://aisel.aisnet.org/misq/vol43/iss2/13/

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), pp. 1–20. Also available at https://aisel.aisnet.org/misq/vol37/iss1/2/

Wright, R. T., Johnson, S. L., and Kitchens, B. (n.d.). "Phishing Susceptibility in Context: A Multi-Level Information Processing Perspective on Deception Detection," *MIS Quarterly* (Forthcoming).

Yoo, C. W., Goo, J., and Rao, H. R. 2020. "Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness," *MIS Quarterly* (44:2), pp. 907–931. Also available at https://aisel.aisnet.org/misq/vol44/iss2/15/

Yue, W. T., Wang, Q.-H., and Hui, K.-L. 2019. "See No Evil, Hear No Evil? Dissecting The Impact of Online Hacker Forums," *MIS Quarterly* (43:1), pp. 73–95. Also available at https://aisel.aisnet.org/misq/vol43/iss1/6/