A Qualitative Multi-Method Study of U.S. Banks’ Financial Reporting Addressing Security Risk Management (SRM) Operational Effectiveness and SRM Maturity

Angela G. Jackson-Summers
U.S. Coast Guard Academy

Security risk management (SRM) presents continued challenges for IT executives. Because of growing data breaches, significant funding needs, and non-stop malicious cyber threats, SRM operational effectiveness and SRM maturity present ever-changing complexities. In organizations, cyber-related events, including advancing information technologies, contribute to the increasing complexity and guarded nature of SRM. This qualitative study was designed to examine SRM operational effectiveness and SRM maturity in financial reporting. Using a set of qualitative techniques, a sample of 107 SRM financial reported statements were rendered from 1,113 U.S. banks’ financial reporting artifacts. Validation of results involved interviews and Q-sorting among three Chief Information Security Officers (CISOs) as subject matter experts. This study presented evidence of varying perceptions of SRM operational effectiveness and SRM maturity were conveyed that may or may not properly reflect how well organizations may perform against cyber-related events. To researchers, practitioners, and policymakers, this study offers an alternative approach and theoretical considerations for future SRM research, especially when reporting cyber-related events.

Keywords: security risk management (SRM), directed content analysis, textual analysis, Q-sorting, provisional coding

INTRODUCTION

Since 2014, cybersecurity has been ranked as the top ranked “most important or worrisome IT management issue” among information technology (IT) leadership (Johnson et al., 2024). In 2023, while 44.5% of 436 IT leaders regarded cybersecurity as being “most important or worrisome IT management issue”, 39.0% conveyed that cybersecurity garnered the largest share of IT organizational investments and 29.1% stated that more investments should be made (Johnson et al., 2024) to help strengthen cybersecurity capabilities. However, the number of data breaches, most caused by malicious cyber attacks, impacting various companies, and associated costs have continued to increase (IBM Security, 2023; Ponemon Institute, LLC, 2022). In organizations, having the technical skills related to cybersecurity are important, but most difficult to find as reported by 47.7% and 45.4% IT leaders, respectively (Johnson et al., 2024). While information technology investments are procured to help address cybersecurity concerns, security risk management (SRM) is crucial in addressing information security.

With the Securities and Exchange Commission (SEC) publishing new cybersecurity disclosure requirements on July 26, 2023, impacting public companies that are subject to the Securities Exchange Act of 1934 reporting requirements (U.S. Security and Exchange Commission, 2023), a greater focus of SRM maturity and effectiveness is needed. These new cybersecurity disclosure requirements state that cybersecurity incidents deemed 'material' must be disclosed by filing Form 8-K. Additionally, disclosures addressing "cybersecurity risk management, strategy, and governance" must be reported on an annual basis using Form 10-K whereas foreign private issuers (FPIs) would file using Form 6-K and Form 20-F, respectively in similar financial reporting events (U.S. Security and Exchange Commission, 2023). Prior to this new SEC publication, disclosure guidance relating to cybersecurity incidents and risks was provided by the SEC's Division of Corporation Finance to support periodic financial reporting and disclosure requirements (Division of Corporation Finance, 2011). Prior to 2023, financial reporting of cybersecurity incidents has reflected minimal filing of cybersecurity incident disclosures and rendered written statements relating to organizational SRM processes, policies, or activities performed that may have been misinterpreted.

SRM provides a continuous way to protect information through the efforts of risk identification and prioritization (Spears & Barki, 2010). To safeguard information, the effectiveness of SRM encompasses a set of specifically, designed controls (Spears & Barki, 2010). The maturity level of the SRM process affects its execution (Spears et al., 2013), which is reliant upon such controls. To help address prior and potential future financial reporting cybersecurity-related disclosure concerns, the following research questions are being posed with this study of the living world of SRM.

RQ1. *What have previously reported written statements relating to the SRM operational effectiveness conveyed?*

RQ2. *What have previously reported written statements relating to SRM maturity conveyed?*

The motivation for this paper is fostered by the importance of SRM in organizations. This paper's purpose intends to address the above research questions, and to heighten research awareness and need for qualitative multi-method approaches when examining SRM due to its complex, advancing, and ever-changing nature, including self-guarded organizational environment.

The Theoretical Foundation and Capability Maturity Model

SRM involve controls consisting of "policies, procedures, safeguards, and countermeasures that prevent, detect, or minimize an information systems security breach" (Spears & Barki, 2010, p. 504). To address information security risks, controls are designed, implemented, and monitored (Spears & Barki, 2010) to help address their operational effectiveness. SRM and related controls organizationally exist. The maturation of the SRM organizational process is necessary to counter security threats (Spears et al., 2013). Additionally, firm outcomes of perceived compliance and actual security performance are additionally impacted by the organizational maturity and relationships among security resources (Kwon & Johnson, 2013).

In early literature, studies focused on evaluating information security studies and posing recommendations for future research (Dhillon & Backhouse, 2001; Siponen, 2005; Zafar & Clark, 2009) have been performed. SRM related studies have been minimal (Zafar & Clark, 2009), especially when focused on SRM effectiveness as an organizational process, including its capabilities and maturity towards improved effectiveness. Maturity of SRM practices can also affect perceived confidence and trust in an organization's security effectiveness. The effectiveness of security operations is driven by the assurance that organizational security requirements have been satisfied (Spears et al., 2013). Security confidence and trust supported by organizational actions or statements indicate that certain levels of SRM maturity are in place (Spears et al., 2013). As a result, SRM maturity and effectiveness have essential roles in driving firm performance.

The Resource-Based View Theory

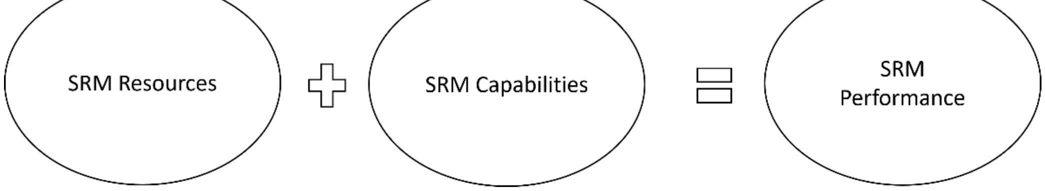
Rooted in strategic management literature, the premise of the RBV theory is that a firm's resources and capabilities contribute to firm performance (Barney, 1991; Wernerfelt, 1984). The foundation of this research work relied upon the combined use of the resource-based view (RBV) theory and a capability maturity model framework. In the RBV theory, firm resources can be defined in several ways. In early literature, a resource was defined as "anything which could be thought of as a strength or weakness of the firm" (Wernerfelt, 1984, p. 172). In information systems security literature, security resources include "security personnel, information technology security applications, physical/technical equipment, or security procedures or policies" (Kwon & Johnson, 2013, p. 44). Information technology security resources, their capabilities, and security controls, such as policies and procedures, strengthen information security throughout business operations when consistently practiced (Kwon & Johnson, 2013). High operational maturity of firms is a factor when examining the planning and implementation activities of security resources (Kwon & Johnson, 2013).

Resource capabilities can be strategic, enabling, operational, and supplemental in nature (Karimi et al., 2007). Resource capabilities allow firms to remain strategically integrated and operationally aligned (Hendersen & Venkatraman, 1999). Strategic alignment, which address the level of fit or coordination extended in aligning business and information technology strategies (Chan & Reich, 2007; Tallon, 2010). These resource capabilities are derived from firm processes that work to integrate and deploy their resources towards their intended purpose or value (Bharadwaj, 2000). The vigor of resource capabilities is linked to firm performance (Santhanam & Hartono, 2003). The extent of resource capabilities resulting from a firm's ability to obtain, implement, and control information technology resources can lead to firm performance (Bharadwaj, 2000; Stoel & Muhanna, 2009; Wang et al., 2012). Security resource capabilities have synergistic value, and they support positive firm outcomes (Kwon & Johnson, 2013).

While firm performance is often measured in terms of organizational financial outcomes, other measures to evaluate firm performance exist when security resources and security resource capabilities are involved. Firms having greater information technology capability outperform other firms (Bharadwaj, 2000; Santhanam & Hartono, 2003; Teo & Ranganathan, 2003). Firm performance is dependent upon its collective resources and their capabilities (Teo & Ranganathan, 2003). Permutations of high uniqueness and low inimitability among resources play a role in strategic advantages positively impacting firm performance (Teo & Ranganathan, 2003). The sustainability of benefits from information technology resource capabilities is expected (Santhanam & Hartono, 2003). Knowing that resource capabilities can be viewed as key drivers of firm performance (Wade & Hulland, 2004), variations in organizational performance are described in terms of its resource types and capabilities (Stoel & Muhanna, 2009). The actual security that takes place when breaches occur can be measured as a form of firm performance (Kwon & Johnson, 2013). The ability to comply with regulatory requirements can also be measured as a firm performance outcome (Kwon & Johnson, 2013).

FIGURE 1
THE RESOURCE-BASED VIEW THEORETICAL LENS TO SECURITY RISK MANAGEMENT (SRM)

An Adaptation of the RBV Theory



Using the RBV theory, relationships among security resources used to safeguard information, and firm outcomes of perceived compliance and actual security performance have been examined (Kwon & Johnson, 2013). Organizational maturity and relationships among security resources effect firm outcomes, such as actual security and compliance (Kwon & Johnson, 2013). Use of the RBV theory helped to further examine SRM maturity and effectiveness towards firm performance.

The Capability Maturity Model (CMMI-SVC)

The Capability Maturity Model (CMM) provides structure and industry-accepted practices for process improvement (Siponen & Willison, 2009). For process advancement, the capability maturity model framework was created by the Software Engineering Institute (SEI) at Carnegie Mellon University (Spears et al., 2013). CMM is represented by many models of which each has a specific purpose, goals, and targeted capability and maturity levels (Team, 2010).Information security literature strongly advocates the use of the Systems Security Engineering – Capability Maturity Model (SSE-CMM) (Siponen & Willison, 2009). The SEI Capability Maturity Model Integration (SEI-CMMI) framework is considered more appropriate when assessing a process that emphasizes information systems and business driven process capabilities (Gu & Jung, 2013). Processes assessed using the SEI-CMMI framework help support organizational goals (Gu & Jung, 2013).

The SEI-CMMI framework includes three models: CMMI for Acquisition (CMMI-ACQ), CMMI for Development (CMMI-DEV), and CMMI for Services (CMMI-SVC) (Team, 2010). Of the three models, the CMMI-SVC offered best practices for ‘quality service delivery’ (Team, 2010). The CMMI-SVC model is comprised of twenty-four process areas, which can be used individually or in combination to assess a process and identify improvement opportunities towards maturity (Team, 2010). While the CMMI-SVC process area, Risk Management (RSKM), has not been widely used in information systems literature, it offered an ‘integrated’ process model for an organizational process, such as SRM.

The RSKM process area was selected due to SRM conveyance in prior literature and written statements (i.e., involvement of individual and cross-organizational process areas). Table 1 below shows both the capability levels and maturity levels as defined by the SEI-CMMI SVC RSKM framework. With the SEI-CMMI SVC RSKM framework, capability levels relate to individual process areas, and maturity levels relate to cross-organizational process areas (Team, 2010), which are regarded as the internal and external organizational SRM process activities, respectively, in this study.

TABLE 1
THE SOFTWARE ENGINEERING INSTITUTE’S CAPABILITY MATURITY MODEL INTEGRATION FRAMEWORK SERVICES – RISK MANAGEMENT PROCESS (SEI-CMMI SVC RSKM)

Capability Levels		Maturity Levels	
0	(Incomplete) – Partially performing or not performing (Team, 2010)	1	(Initial) – Achieving organizational process goals in an unstructured way (Team, 2010)
1	(Performed) – Accomplishing the required work (Team, 2010)		
2	(Managed) – Performing process in accordance with policy (Team, 2010)	2	(Managed) – Governing the organizational process using a formal, structured approach (Team, 2010)
3	(Defined) – Managing process in an organizational tailored fashion (Team, 2010)	3	(Defined) – Maintaining and continuously improving the organizational process (Team, 2010)

In the next section, the study’s qualitative, multi-method approach is described. Afterwards, in the Discussion section, the results as well as interpretations of data are presented. Lastly, I close with the implications of this study to practice, research, and policy.

METHODOLOGY

Qualitative exploration extends a long-term research approach (Stebbins, 2001) to SRM, especially considering its nature of being highly complex and highly guarded amid an ever-changing social and advancing information technological environment. Qualitative research provides a real-world view, especially from individuals, of the how and why perspectives of the phenomenon of interest exist (Cassell & Symon, 2004), and it offers richness and transparency in telling the story of a phenomenon given the quality and comprehensiveness of the study (Bansal & Corley, 2012). This qualitative SRM exploration was grounded on the resource-based view (RBV) theory when examining the SRM process, and the Software Engineering Institute's Capability Maturity Model Integration (SEI-CMMI) framework when examining SRM operational effectiveness and SRM maturity.

Sample

Using a set of qualitative techniques, a sample of 107 SRM financial reported statements were rendered from 1,113 U.S. banks' financial reporting artifacts. The qualitative techniques included the performance of a directed content analysis, text mining and text analysis using two automated tools, Provalis Research's qualitative data analysis (QDA Miner) and WordStat software. SRM content from a sample of 1,113 financial reporting artifacts from ten (10) U.S. banks was examined using the directed content analysis (DCA) approach. Using a DCA approach is beneficial when alternatively seeking to collect and interpret data absent of direct study participant engagement (Hsieh and Shannon, 2005). Next, the identification and collection of the study's artifacts are described.

Identification and Collection of Study's Artifacts

Because the banking industry has been highly regulated requiring reporting of security breaches (U.S. Securities and Exchange Commission, 2011), ten U.S. banks were randomly selected to identify and collect this study's artifacts for review. In a prior qualitative, interpretive study, we noted the basis of the study was grounded on the Sarbanes-Oxley Act (SOX) causing firms to make significant investments (Spears et al., 2013) for regulatory compliance in firms' financial reporting. The reliability of financial reporting became a heightened objective for regulatory compliance to SOX (Spears et al., 2013). In review of financial reporting documents for this study, the U.S. banks' artifacts, were identified based on solicited feedback from a Chief Accounting Officer at a Fortune 500 company. In the case of a major firm event, such as a cyber-attack or other security occurrence, organizations are required to disclose such occurrences, and their related financial or operational events (U.S. Securities and Exchange Commission, 2011). The identification and collection of artifacts covered the inception of SOX regulatory compliance in 2005 through the annual financial reporting period ending December 31, 2016. Table 7 below provides a listing of the organization artifacts that were used in the content analysis. The random sample size of ten (10), 8 active and 2 inactive, out of 757 total U.S. commercial banks determined by using the University of Pennsylvania's Wharton Research Data Services (WRDS) Audit Analytics database as of May 17, 2017.

TABLE 2
ARTIFACTS AND TARGETED CONTENT FOR DIRECTED CONTENT ANALYSIS FOR THE PERIOD OF JANUARY 1, 2005 – DECEMBER 31, 2016

Form Type	Section Title(s)
10-K	Part I. Item 1A. Risk Factors Part I. Item 3. Legal Proceedings Part II. Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations Part II. Item 9A. Controls and Procedures
10-Q	Part I. Item 2. Management's Discussion and Analysis of Financial Condition and Results of Operations Part I. Item 4. Controls and Procedures Part II. Items 1A. Risk Factors Part II. Items 1. Legal Proceedings
8-K	Item 8.01 Other Events

For each of the 10 U.S. banks, three types of forms, 10-K, 10-Q, and 8-K, filed with the Security Exchange Commission (SEC) covering the fiscal year periods 2005 through 2016 were collected. The SEC maintains and allows access to such filings on their Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system located at https://www.sec.gov/edgar.shtml. A total of 1,079 artifacts collected for the 10 U.S. banks were downloaded and loaded into QDA Miner.

After loading the 1,079 artifacts, each file was reviewed to identify the specific form sections that related to security using the security code and its related keywords. Of the 1,079 artifacts, 45 10-Ks and 136 10-Qs failed to be read by QDA Miner, because of optical character recognition (OCR) issues. The failed artifacts were converted into other formats (i.e., PDF to MS Word) using the Internet document conversion tool, PDF2GO.com, and reloaded. While reviewing each loaded artifact, 43 supporting documents referenced as Exhibits were collected and loaded. Upon review of the loaded artifacts, some of the artifacts contained data exceptions (i.e., duplicate filing). The artifacts that contained data exceptions were examined, removed, and replaced with the correct artifacts, if required. In QDA Miner, each loaded artifact is regarded as a case. Upon completion of data preparation and error handling, a total of 1,113 cases resulted. For a breakdown of the total QDA Miner cases loaded in QDA Miner, see Appendix A.

Data Coding and Analysis

From the collection of artifacts, the design and development of codes to apply and filter the content were both manually and automatically performed. Content coding was necessary to perform the directed content analysis (DCA).

Code Design and Development (Manual vs Automated Coding)

The design and development of codes were based on my study's RBV-based operational model as shown in Figure 1. Codes were designed for each construct: SRM, SRM security resources, SRM security capabilities, firm performance, as well as each capability level and each maturity level of the CMMI-SVC RSKM model. The initial efforts in code design and development involved the identification of keywords that would define each code. The keywords that were manually-developed resulted in a total of 498 keywords.

When compared to manually-driven content analysis, an automated approach has been proven to be reliable and advantageous (Bortiz et al., 2013). An automated approach to content analysis using tools, such as QDA Miner, provides advancements in building word dictionaries, ease of coding changes and combined use of text retrieval, and coding consistency, replication, and scalability (Bortiz et al., 2013). Also, for exploratory studies when taking an automated approach, provisional coding is a technique that helps to establish codes, and additional refinement of such codes as content analysis progresses (Saldana, 2013).

Using an automated approach to DCA, provisional coding was adopted and applied. The provisional coding technique allows pre-defined codes or coding definitions to be established through prior research findings and other related literature (Saldana, 2013). With provisional coding, prior literature definitions were reviewed and captured in WordStat for the key term of security and each of the study's constructs.

Using the WORD FREQUENCY feature in WordStat against each of the definitions, specific keywords were identified. See Appendix B for the full listing of all key terms and constructs, including their respective definitions captured from prior literature, and the dictionary keywords that resulted. Code development supporting the DCA was comprised of all the keywords defined. As a result, 107 financial reported statements were captured.

.

Integrity Measures

In executing the inter-rater reliability (IRR) check, two significant challenges were experienced during data coding and analysis. The first challenge related to the presence of possible bias and subjectivity in the manual coding design and development effort resulting in the collection of 498 keywords. The second challenge resulted from the efforts of reaching a reasonable agreement in the 498 keywords. Two academic security subject matter experts (SMEs) having over ten years of security experience performed the IRR check. Using literature-based definitions and their own real-world experiences, each SME was requested to review each manually-defined keyword and align them to the study's constructs. The overall results of the IRR check showed a difference of 22.89% between the SMEs. Additionally, one of the SMEs voiced confusion and being uncomfortable when performing the IRR, because of the large volume of keywords. With such a difference in the IRR check and consideration of the SME's feedback of discomfort in performing the IRR, the automated approach in defining codes, including related keywords, was applied.

Data Management

Each of the 107 financial reported statements were captured on individual index cards to support the facilitative performance of a Q-sort validation process in identifying SRM operational effectiveness via the specific capability levels and SRM maturity via the specific maturity levels defined by the SEI-CMMI SVC RSKM framework. Three SRM experts who were in the role of Chief Information Security Officer (CISO) or an equivalent company position agreed to participate in the Q-sorting efforts. The Q-sort technique when used in smaller participant numbers can purposefully support certain complexities and distinctions when examining data (Watts and Stenner, 2005). Each SRM expert was separately requested to review and categorize each SRM financial reporting statement by capability level and maturity level.

Additionally, interviews were also performed of the SRM experts at the close of the Q-sorting efforts to gather additional feedback on the results and their conveyance. Qualitative interviews are viewed as one of the most significant tools for data collection in qualitative research (Myers & Newman, 2007). Qualitative interviews previously have been simplistically viewed, and researchers need to be aware of the issues and pitfalls that can result in potential risks in the quality of studies performed (i.e., incomplete data) (Myers & Newman, 2007). To address the problems and pitfalls of the qualitative interview, Myers and Newman (2007) suggested that it be viewed as a 'social exchange' in a dramatic theatrical setting involving actors and behavioral expectations.

DISCUSSION

Conceptual insights to SRM operational effectiveness and SRM maturity were gained from this study's results. Also, the directed content analysis process, including text mining and textual analysis provided three key outcomes: (1) the SRM presence in financial reporting statements, (2) the development of an SRM-focused dictionary, and (3) analysis results of the sample of 107 financial reporting statements for this study. This study's research questions were fully addressed through the analysis and validation efforts performed against the sample of 107 financial reporting statements.

SRM Presence

SRM presence in financial reporting statements was evidenced during the period of 2005 through 2016. Table 2 below provides trending of SRM content in financial reporting statements. The growing presence of SRM content may have been a response to organization required regulatory compliance to the Sarbanes-Oxley Act (SOX). It was noted that of the two inactive banks included in the study's sample, only 1 of the 2 inactive banks had SRM content present in their financial reporting statements during the perioding of 2007 through 2016.

TABLE 2
SRM CONTENT PRESENCE IN FINANCIAL REPORTING STATEMENTS

	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
No. of Banks	1	2	3	3	3	2	5	7	8	8	8	8

SRM-Focused Dictionary

As shown in Appendix B, the RBV-based theoretical framework and CMMI-SVC RSKM model both helped to establish an SRM-focused dictionary that supported the DCA of the SRM financial reporting statements. The supporting statistical information relating to the study's coded constructs' consisting of defined keywords are shown below in Table 3. The *TF • IDF* represents *Term Frequency Weighted by Inverse Document Frequency* which assumes that the coded construct becomes more representative of its content as it occurs more in an artifact, such as a document.

TABLE 3
CONSTRUCTS' KEYWORDS' FREQUENCIES AND OTHER STATISTICS (RANKED IN FREQUENCY ORDER)

	FREQUENCY	TF • IDF
SRM	1,818	5,542.1
MAT_LVL_2	1,322	4,030.0
SEC_CAP	821	2,502.8
SEC_RES	712	2,170.5
FIRM_PERF	645	1,966.2
CAP_LVL_3	295	899.3
CAP_LVL_2	256	780.4
CAP_LVL_1	255	777.4
MAT_LVL_3	98	298.7
CAP_LVL_0	14	42.7
MAT_LVL_1	12	36.6

Directed Content Analysis (DCA) Results

During the validation of DCA results by the three SRM experts, one of the experts expressed concern with the transparency of existing financial reporting statements accurately reflecting organizational SRM. This SRM expert did not participate in the Q-sort validation exercise. The SRM expert openly shared views on governance and SRM resources, especially the importance of SRM framework use and preferential use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

The remaining two SRM experts completed the Q-sort validation exercise, and their results were captured as shown below in Table 4. The completed DCA efforts yielded SRM financial reported statements that were assessed against the CMMI-SVC RSKM model. Each of the SRM financial reported statements was assigned a specific capability level and specific maturity level (pairing) from the CMMI-SVC RSKM model by each SRM expert. For a listing of all 107 SRM financial reported statements, refer to Appendix D.

TABLE 4
SUMMARY OF SRM Q-SORT VALIDATION RESULTS

Capability Levels	Maturity Levels	Respondent 1	Respondent 2
Not Assigned	Not Assigned	3	0
0 (Incomplete)	None	0	0
0 (Incomplete)	1 (Initial)	4	50
0 (Incomplete)	2 (Managed)	0	0
0 (Incomplete)	3 (Defined)	0	0
1 (Performed)	None	0	0
1 (Performed)	1 (Initial)	17	29
1 (Performed)	2 (Managed)	25	4
1 (Performed)	3 (Defined)	4	0
2 (Managed)	None	0	0
2 (Managed)	1 (Initial)	5	0
2 (Managed)	2 (Managed)	20	17
2 (Managed)	3 (Defined)	19	1
3 (Defined)	None	0	0
3 (Defined)	1 (Initial)	0	0
3 (Defined)	2 (Managed)	2	0
3 (Defined)	3 (Defined)	8	6
		107	107

SRM Operational Effectiveness Conveyed

The DCA did reflect a very strong presence of SRM in financial reporting statements when compared to all other coded constructs. The keywords associated with SRM and firm performance (FIRM_PERF) appeared 96% throughout the SRM financial reporting statements. In review of prior SRM financial reporting statements, there was no content present of actual data breaches or cyber attacks being reported in compliance with regulatory requirements.

In review of Table 3, the CMMI-SVC RSKM capability levels 1-3 captured as CAP_LVL_1, CAP_LVL_2, and CAP_LVL_3 were present within the SRM financial reporting statements. In Table 4, SRM experts had varying perspectives on the presence of all CMMI-SVC RSKM capability levels. The presence of the RSKM capability levels evidences SRM operational effectiveness. Additionally, the presence of RSKM capability levels further supports the theoretical applicability of the adapted RBV theoretical model as originally depicted in Figure 1 in financial reporting statements. As a result, I propose the following:

P1. *The internal SRM process is positively related to SRM resources.*

P2. *The internal SRM process is positively related to SRM capabilities.*

P3. *SRM performance is positively related to the internal SRM process.*

SRM Maturity Conveyed

When considering SRM maturity, Table 3 above showed dominant presence of CMMI-SVC RSKM maturity level 2 coded as MAT_LVL_2. In Table 4, SRM experts had varying perspectives on the presence of all CMMI-SVC RSKM maturity levels, especially MAT_LVL_1 and MAT_LVL_2. These varying perspectives on the CMMI-SVC RSKM maturity levels suggest differences in how SRM maturity may influence or impact SRM performance. As a result, I propose the following:

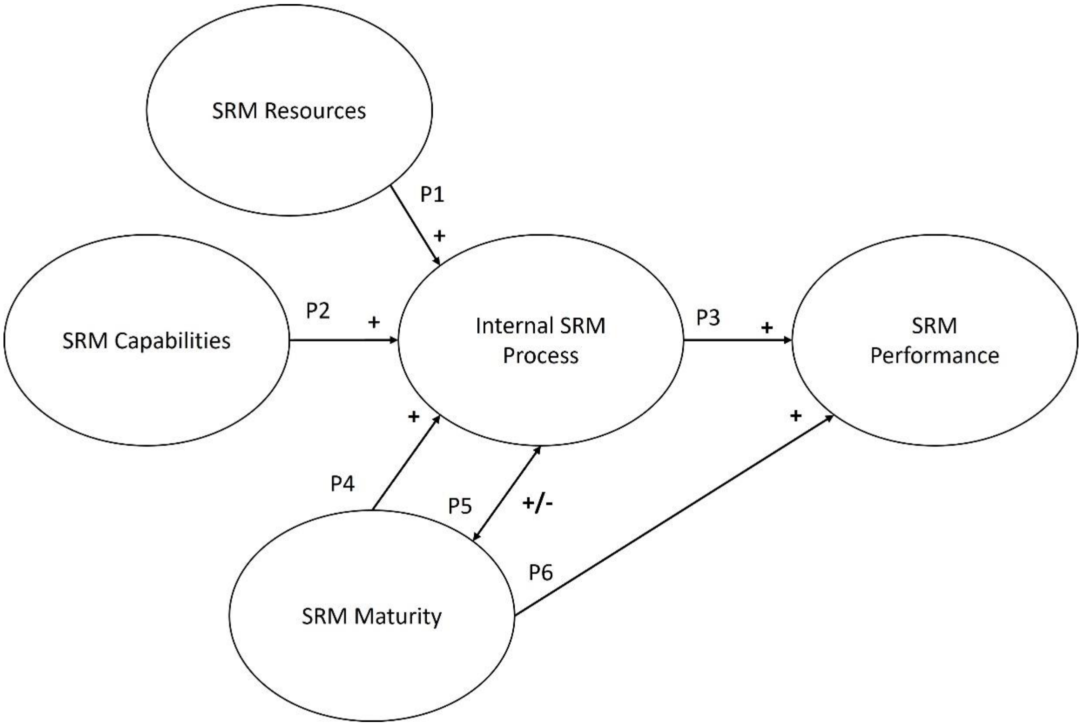
P4. *The internal SRM process is positively related to SRM maturity.*

P5. *Due to SRM maturity, the internal SRM process may positively (or negatively) influence SRM performance.*

P6. *SRM performance is positively related to SRM maturity.*

The study's proposed conceptual model is shown below in Figure 2.

FIGURE 2
SRM PROPOSED CONCEPTUAL MODEL



Limitations

There were several limitations to this study. One key limitation involves a study's use of directed content analysis. With the use of theory, such as the RBV theory, informed, strong bias can exist among researchers causing researchers to seek supportive versus non-supportive evidence of the theory used. Also, overemphasis of the theory can blind researchers to the contextual aspects of the research phenomenon.

Generalizability issues can result from differences that might exist among SRM practices, varied security resource portfolios, and a firm's structure, culture, and leadership. Because of the various concepts covered throughout this study, the understanding of terminology, concepts, and techniques presents another limitation.

The sample of CISOs represented three different U.S. industries: retail, telecommunications, and banking. Because the CISO who worked in the U.S. banking industry did not complete the validation exercise of the SRM financial reported statements, the feedback received from the remaining two CISOs could be viewed as a study limitation. This limitation relates to the CISOs having varied experiences in the financial reporting disclosure requirements that may differ from a CISO working in a highly regulated industry, such as banking.

When considering the sample of artifacts involving financial reporting statements in the banking industry, differences in the extent of conveyed SRM practices and incidents might exist. Such differences do reflect less importance of SRM when compared among industries, but these differences could indicate differences in resources and their capabilities among organizations. For example, one CISO mentioned that the level of funding approved to support SRM would perceivably be less than a bank due to banks being highly regulated. So, the extent of SRM financial reporting statements among industries may reflect differences in similar research studies.

Inconsistency among banks in how and where SRM content is documented in their respective financial reporting statements housed on the EDGAR database exist. For some banks, SRM content was stored in other referenced documents, which were labelled as Exhibits. These inconsistencies created challenges in locating and extracting SRM content to be loaded for the directed content analysis work.

Lastly, for this study, the limited accessibility of CISOs and willingness to participate were challenges in identifying a sample size in the time frame previously planned. When soliciting CISOs to participate in my study, several CISOs inquired with concern about the privacy of their company's security information and were reluctant to participate. Overcoming such challenges creates a limitation in achieving larger sample sizes among security executives to participate in research studies when involving security.

IMPLICATIONS

The results of this study extended the RBV-based view theoretical model with the consideration of SRM process capability levels and SRM process maturity and tailored the RBV-based view theory to specifically address the SRM organizational process. The use of artifacts, such as financial reporting statements, was an alternative approach to examine the SRM phenomenon giving the continued growing concerns to address data breaches and cyber attacks. Because prior research has noted security related studies as being highly guarded, this alternative study's approach offered a least intrusive research approach. Overall, this study is intended to contribute future research opportunities and considerations among researchers, practitioners, and policymakers when addressing SRM-related financial reporting statements.

Research

This study offers future research opportunities when addressing the SRM process using other theories, such as institutional theory or process theory. There are also challenges that may suggest additional research on SRM leadership dynamics, and the use of differing frameworks or policies. Among CISOs, their beliefs and experiences may influence how they view SRM operational effectiveness and SRM maturity as well as SRM performance. Lastly, when examining SRM in less regulated industries, other alternative research methods may be considered and proven to offer better research approaches in expanding SRM exploration.

Practice

In the living world of SRM, organizations' SRM resources, SRM capabilities, and SRM performance vastly differ. This study may suggest future considerations in how financial reporting not only captures cyber events when they occur, but also balance the messaging of their organizational SRM process with emphasis on SRM operational effectiveness and SRM maturity. With U.S. banks, federal regulations also address brand management and consumer trust as focal concern areas, when addressing security and privacy events.

Policy

With the publication of the (U.S. Security and Exchange Commission, 2023), the reporting of cyber events is required. Throughout the study's sample period, there was no evidence of cyber events occurring between 2005 and 2016 for the U.S. banks selected. Prior financial reporting statements did show evidence of SRM content. However, the SRM content did not consistently reflect SRM operational effectiveness or SRM maturity levels in financial reporting statements. This lack of consistency or structure could pose challenges among readers of financial reporting statements as demonstrated among the varying perspectives gained in this study. Future considerations may suggest additional guidance in balancing the financial reporting of cyber events, SRM operational effectiveness, and SRM maturity, especially for investor purposes.

REFERENCES

Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and internet security breaches. *Communications of the Association for Information Systems*, *12*(1), 684–700.

Bansal, P., & Corley, K. (2012). Publishing in AMJ—Part 7: What's different about qualitative research? *Academy of Management Journal*, *55*(3), 509–513.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120.

Bharadwaj, A.S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly*, *24*(1), 169–196.

Boritz, J.E., Hayes, L., & Lim, J.-H. (2013). A content analysis of auditors' reports on IT internal control weaknesses: The comparative advantages of an automated approach to control weakness identification. *Internal Journal of Accounting Information Systems*, *14*(2), 138–169.

Brown, S.R. (1993). A primer on Q methodology. *Operant Subjectivity*, *16*(3/4), 91–138.

Cassell, C., & Symon, G. (2004). *Essential guide to qualitative methods in organizational research*. (C. Cassell, & G. Symon, Eds.) SAGE.

Chan, Y.E., & Reich, B.H. (2007). IT alignment: What have we learned? *Journal of Information Technology*, *22*(4), 297–315.

Chen, J.-L. (2012). The synergistic effects of IT-enabled resources on organizational capabilities and firm performance. *Information & Management*, *49*(3–4), 142–150.

Chen, P.-Y., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly*, *35*(2), 397–422.

Cohn, M.A., Mehl, M.R., & Pennebaker, J.W. (2004). Linguistic markers of psychological change surrounding September 11, 2001. *Psychological Science*, *15*(10), 687–693.

Cybersecurity & Infrastructure Security Agency. (2020, April 8). *CISA.gov National Cyber Awareness System Alert (AA20-099A): COVID-19 exploited by malicious cyber actors*. Retrieved from https://us-cert.cisa.gov/ncas/alerts/aa20-099a

Debreceny, R.S., & Gray, G.L. (2013). IT governance and process maturity: A multinational field study. *Journal of Information Systems*, *27*(1), 157–188.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, *11*(2), 127–153.

Dick, P. (2004). Discourse analysis. In C. Cassell, & G. Symon (Eds.), *Essential guide to qualitative methods in organizational research* (pp. 203–213). SAGE.

Division of Corporation Finance. (2011, October 13). *CF disclosure guidance: Topic no. 2*. Retrieved from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Goel, S., & Chengalur-Smith, I.N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, *19*(4), 281–295.

Gu, J.-W., & Jung, H.-W. (2013). The effects of IS resources, capabilities, and qualities on organizational performance: An integrated approach. *Information & Management*, *50*(2–3), 87–97.

Hendersen, J.C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *38*(2–3), 472–484.

Hsieh, H.-F., & Shannon, S.E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288.

IBM Security. (2023). *Cost of a data breach report 2023*. Armonk, NY: IBM Corporation. Retrieved from https://www.ibm.com/reports/data-breach

Johnson, V., Maurer, C., Torres, R., Guerra, K., & Mohit, H. (2024). The 2023 SIM IT issues and trends study. *MIS Quarterly Executive*, *23*(1), Article 7.

Kacewicz, E., Pennebaker, J.W., Davis, M., Jeon, M., & Graesser, A.C. (2014). Pronoun use reflects standings in social hierarchies. *Journal of Language and Social Psychology*, *33*(2), 125–143.

Karimi, J., Somers, T.M., & Bhattacherjee, A. (2007). The role of information systems resources in ERP capability building and business process outcomes. *Journal of Management Information Systems*, *24*(2), 221–260.

Kwon, J., & Johnson, M.E. (2013). Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, *30*(2), 41–65.

Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management Review*, *24*(4), 691–710.

Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research*, 26(3), 565–584.

Mohr, L.B. (1982). *Explaining organization behavior*. San Francisco: Jossey-Bass.

Myers, M.D. (1997). Qualitative research in information systems. *MIS Quarterly*, *21*(2), 241–242.

Myers, M.D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.

Nadkarni, S., & Chen, J. (2014). Bridging yesterday, today, and tomorrow: CEO temporal focus, environmental dynamism, and rate of new product introduction. *Academy of Management Journal*, *57*(6), 1810–1833.

Nevo, S., & Wade, M. (2011). Firm-level benefits of IT-enabled resources: A conceptual extension and an empirical assessment. *The Journal of Strategic Information Systems*, *20*(4), 403–418.

Nevo, S., & Wade, M.R. (2010). The formation and value of IT-enabled resources: Antecedents and consequences of synergistic relationships. *MIS Quarterly*, *34*(1), 163–183.

Pan, G., Pan, S.-L., & Lim, C.-Y. (2015). Examining how firms leverage IT to achieve firm productivity: RBV and dynamic capabilities perspectives. *Information & Management*, *52*(4), 401–412.

Pennebaker, J.W., Chung, C.K., Frazee, J., Lavergne, G.M., & Beaver, D.I. (2014). When small words foretell academic success: The case of college admissions essays. *PloS One*, *9*(12), e115844.

Pfarrer, M.D., Pollock, T.G., & Rindova, V.P. (2010). A tale of two assets: The effects of firm reputation and celebrity on earnings surprises and investors' reactions. *Academy of Management Journal*, *53*(5), 1131–1152.

Ply, J.K., Moore, J.E., Williams, C.K., & Thatcher, J.B. (2012). IS employee attitudes and perceptions at varying levels of software process maturity. *MIS Quarterly*, *36*(2), 601–624.

Ponemon Institute, LLC. (2022). Cost of a data breach report. *IBM Security*.

Pöppelbuß, J., Niehaves, B., Simons, A., & Becker, J. (2011). Maturity models in information systems research: Literature search and analysis. *Communications of the Association for Information Systems*, *29*(27), 505–532.

Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal of Accounting Information Systems*, *20*, 38–64.

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly*, *36*(1), 43–64.

Ravichandran, T., Lertwongsatien, C., & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: A resource-based perspective. *Journal of Management Information Systems*, *21*(4), 237–276.

Reich, B.H., & Benbasat, I. (1996). Measuring the linkage between business and information technology objectives. *MIS Quarterly*, *20*(1), 55–81.

Rhee, E.Y., & Fiss, P.C. (2014). Framing controversial actions: Regulatory focus, source credibility, and stock market reaction to poison pill adoption. *Academy of Management Journal*, *57*(6), 1743–1758.

Sabherwal, R., & Robey, D. (1995). Reconciling variance and process strategies for studying information systems development. *Information Systems Research*, *6*(4), 303–327.

Santhanam, R., & Hartono, E. (2003). Issues in linking information technology capability to firm performance. *MIS Quarterly*, *27*(1), 125–153.

Schultze, U., & Avital, M. (2011). Designing interviews to generate rich data for information systems research. *Information and Organization*, *21*(1), 1–16.

Segars, A.H., & Grover, V. (1998). Strategic information systems planning success: An investigation of the construct and its measurement. *MIS Quarterly*, *22*(2), 139–163.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270.

Siponen, M.T. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems*, *14*(3), 303–315.

Spears, J.L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503–522.

Spears, J.L., Barki, H., & Barton, R.R. (2013). Theorizing the concept and role of assurance in information systems security. *Information & Management*, *50*(7), 598–605.

Stebbins, R.A. (2001). *Exploratory research in the social sciences* (Vol. 48). Thousand Oaks, CA, USA: Sage.

Stoel, M.D., & Muhanna, W.A. (2009). IT capabilities and firm performance: A contingency analysis of the role of industry and IT capability type. *Information & Management*, *46*(3), 181–189.

Tallon, P.P. (2010). A service science perspective on strategic choice, IT, and performance in U.S. banking. *Journal of Management Information Systems*, *26*(4), 219–252.

Tausczik, Y.R., & Pennebaker, J.W. (2010). The psychological meaning of words: LIWC and computerized text analysis methods. *Journal of Language and Social Psychology*, *29*(1), 24–54.

Team, C.P. (2010). *CMMI for Service, Version 1.3, CMMI-SVC v1.3. CMU/SEI-2010-TR-034 Technical Report*. Software Engineering Institute.

Teo, T.S., & Ranganathan, C. (2003). Leveraging IT resources and capabilities at the housing and development board. *The Journal of Strategic Information Systems*, *12*(3), 229–249.

Thomas, D.M., & Watson, R.T. (2002). Q-sorting and MIS research: A primer. *Communications of the Association for Information Systems*, *8*(1), 141–156.

U.S. Security and Exchange Commission. (2023). *Cybersecurity risk management, strategy, governance, and incident disclosure, 17 C.F.R*. Retrieved from https://www.sec.gov/rules/final/2023/33-11216.pdf

Wade, M., & Hulland, J. (2004). The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly*, *28*(1), 107–142.

Wang, J., Gupta, M., & Rao, H.R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. *MIS Quarterly*, *39*(1), 91–112.

Wang, J., Xiao, N., & Rao, H.R. (2015). Research note – An exploration of risk characteristics of information security threats and related public information search behavior. *Information Systems Research*, *26*(3), 619–633.

Wang, N., Liang, H., Zhong, W., Xue, Y., & Xiao, J. (2012). Resource structuring or capability building? An empirical study of the business value of information technology. *Journal of Management Information Systems*, *29*(2), 325–367.

Watts, S., & Stenner, P. (2005). Doing Q methodology: Theory, method and interpretation. *Qualitative Research in Psychology*, *2,* 67–91.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, *5*(2), 171–180.

Zafar, H. (2011). Security risk management at a fortune 500 firm: A case study. *Journal of Information Privacy & Security*, *7*(4), 23–53.

Zafar, H., & Clark, J.G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, *24*(34), 557–596.

Zafar, H., Ko, M.S., & Clark, J.G. (2014). Security risk management in healthcare: A case study. *Communications of the Association for Information Systems*, *34*(37), 737–750.