Strukturierung empirischer Evidenz im Informationssicherheitsmanagement. Vorgehen und erste Ergebnisse.

Danijel Milicevic, Matthias Goeken

IT-Governance-Practice-Network
Frankfurt School of Finance & Management
Sonnemannstr. 9-11
60314 Frankfurt am Main
d.milicevic@fs.de
m.goeken@fs.de

Abstract: Vorhandenes empirisches Wissen zu konsolidieren und für die Forschung sowie das Management der Informationssicherheit zu strukturieren, ist ein Ziel, das sowohl wissenschaftliche als auch praktische Relevanz besitzt. Der Beitrag schlägt ein Vorgehen hierzu vor und präsentiert erste Ergebnisse für einen Ausschnitt der Forschung im weiten Feld des Informationssicherheitsmanagements. So kann gezeigt werden, welche sozialen Faktoren gemäß empirischer Studien die Einhaltung von Richtlinien (Policy Compliance) beeinflussen.

1 Einführung

In der WI-(Wirtschaftsinformatik-), der Information-Systems-Forschung und auch in der Informatik bzw. der Computer-Science-Forschung herrscht nach Ansicht prominenter Forscher ein Mangel an kumulativer Forschung [BZ03; VRG02; Ki09], unter anderem verursacht durch den wenig systematischen Umgang mit vorhandenen Forschungsergebnissen. Dies führt laut Webster und Watson, dazu, dass „the progress of our field is impeded" [WW02]. Card [Ca11] geht sogar soweit festzustellen: „many areas of social science research are in less need of further research than they are in need of organization of the existing research."

Ein wichtiger Aspekt beim Aufbau und Einsatz von verteilten Informationssystemen ist die Gewährleistung von adäquater Informationssicherheit [Mi10]. Gegenstand des Informationssicherheitsmanagements ist die Festlegung von Sicherheitsanforderungen an ein Informationssystem und die Entscheidung in welchem Rahmen Schutzmechanismen eingesetzt werden (in Anlehnung an [Sa11], der allerdings den Begriff IT-Sicherheitsmanagement verwendet). Es wird damit deutlich weiter gefasst als die Herstellung technischer Sicherheit, sondern es geht um eine umfassende Planung, Steuerung und Kontrolle der Informationssicherheit durch organisatorische und technische Maßnahmen. Dies erfordert die Abstimmung mit anderen Managementaufgaben der IT. Das Informationssicherheitsmanagement wird damit auch als Teil der umfassenderen IT-Governance gesehen, die nach diesem Verständnis bspw.

auch IS-Risikomanagement und Business/IT-Alignment umfasst. Zur Gewährleistung von adäquater Informationssicherheit kann die Forschung einen Beitrag unter anderem dadurch leisten, dass vorhandene Forschungsergebnisse konsolidiert und so dem Problemlösungsprozess von praktischen Sicherheitsfragestellungen hinzugefügt werden. Jedoch lässt sich ein Mangel an kumulativer Forschung und bei der Organisation vorhandenen Wissens auch für das Forschungsfeld Informationssicherheitsmanagement konstatieren.

Das Ziel dieses Beitrags ist es daher darzustellen, wie in diesem Feld kumulative Forschung durchgeführt und gestärkt werden kann. Als eine Möglichkeit zum organisierten Umgang mit vorhandenem Wissen und dessen Kumulierung haben sich in anderen Wissenschaftsdisziplinen sogenannte „systematische Reviews“ als vorteilhaft erwiesen (vgl. [Go11], dort auch für eine Übertragung auf die Information-Systems-Forschung). Durch das systematische Zusammentragen von wissenschaftlichen Ergebnissen wird so eine Evidenz für einen vermuteten Zusammenhang hergestellt (Evidenz im Sinne von Beweis und Nachweis, wie es in der Evidenzbasierten Medizin Verwendung findet).

Um Ablauf und mögliche Ergebnisse sowie den Nutzen systematischer Reviews aufzuzeigen, werden für einen Ausschnitt der Forschung zum Informationssicherheitsmanagement - die Einhaltung von Richtlinien (Policy Compliance) -, konkrete Ergebnisse präsentiert und diskutiert.

Der Beitrag ist wie folgt aufgebaut: In Abschnitt 2 werden Grundlagen zur Forschung im Informationssicherheitsmanagement sowie zu Literaturreviews, systematischen Reviews und deren Ablauf diskutiert. Der darauffolgende Abschnitt 3 stellt die einzelnen Aktivitäten des durchgeführten Reviews dar und präsentiert dessen Ergebnisse. Im Anschluss wird ein Fazit gezogen und es wird kurz der Nutzen von systematischen Reviews für die Informationssicherheitsmanagement-Forschung aus einer übergreifenden Perspektive diskutiert. Abschließend wird weiterer Forschungsbedarf aufgezeigt.

2 Grundlagen

2.1 Forschung zum Informationssicherheitsmanagement

Die Forschung zum Informationssicherheitsmanagement ist geprägt von konzeptionellen und technischen sowie theoretischen Arbeiten, die sich im Wesentlichen subjektiv-argumentativer Methoden bedienen. Empirische Arbeiten und Arbeiten, die vorhandene konzeptionelle und technische Artefakte und Produkte evaluieren, insbesondere vergleichend evaluieren, finden sich hingegen in weitaus geringerer Anzahl [SWB08]. Allerdings zeigen durchgeführte Literatursuchen in Literaturdatenbanken und -portalen (siehe Abschnitt 3), dass sich eine gewisse Anzahl empirischer Arbeiten finden lässt, die für einen systematischen Review eine ausreichende Grundlage bilden. Aktuell sind den Verfassern keine entsprechenden systematischen Reviews zum Thema Informationssicherheitsmanagement bekannt, die für den Aufbau einer empirisch fundierten, kumulierten und zweckmäßig organisierten Wissensbasis herangezogen werden könnten.

Hieraus ergibt sich, dass Wissenschaftler nur schwer einen Überblick darüber bekommen können, für welche Fragestellungen des Forschungsfeldes bereits Studien und damit Wissen im Sinne von „empirischer Evidenz“ vorliegen bzw. wo eben dieses fehlt. Zum anderen können sich Entscheidungen in der Praxis (beispielsweise solche, die die Beurteilung der Vorteilhaftigkeit von Maßnahmen (bspw. Schutzmechanismen) betreffen oder die Relevanz von Faktoren, die die Informationssicherheit beeinflussen) nicht auf aufbereitete empirischer Evidenz stützen.

2.2 Traditionelle Literaturreviews und Systematische Reviews

In der Informatik, der WI- und auch in der IS-Forschung finden sich seit einiger Zeit vermehrt Kritik zu herkömmlichen, sogenannten traditionellen Reviews und damit einhergehend Anregungen für bzw. Forderungen nach einem systematischerem Vorgehen bei der Anfertigung von Literaturübersichten und Reviews, die jedoch bislang nur im geringen Maße aufgegriffen wurden [MS07; Br09; Oa11]. Ein wesentliches Merkmal Systematischer Reviews ist, dass sie einem festgelegten Vorgehensmodell (häufig auch als „Protokoll“ bezeichnet) folgen (Abbildung 1 und [Go11] für eine Übersicht verschiedener Vorgehensmodelle). Hierdurch soll das Vorgehen transparent und grundsätzlich reproduzierbar sein, was die Glaubwürdigkeit der Reviewergebnisse erhöhen soll [Oa11].

In der Kritik stehen die traditionellen Reviews, da sie zumeist eine breite Forschungsfrage der Art “what is known about X” [Go09] zugrunde legen. Für Systematische Reviews wird hingegen empfohlen, eine enge und fokussierte Forschungsfrage zu wählen und vorhandene Forschungsergebnisse dazu zu nutzen, diese zu beantworten bzw. konfligierende Forschungsergebnisse mit Blick auf die Forschungsfrage aufzuzeigen.

Aktivitäten
1. Definition der Forschungsfrage
2. Suche nach relevanten Studien in der Primärforschung
3. Evaluation und Entscheidung über Einschluss/Ausschluss
4. Analyse der Ergebnisse der Primärforschung mit Blick auf die Forschungsfrage
5. Zusammenfassung (Integration/Synthese) der Ergebnisse
6. Diskussion

Abbildung 1: Vorgehensmodell für ein Systematisches Review [Go11]

Darüber hinaus wird für *systematische* Reviews gefordert, dass der Prozess der Literatursuche (Aktivität 2) transparent und reproduzierbar ist und nach Möglichkeit alle verfügbaren Quellen relevanter Forschungsergebnisse genutzt werden. Ebenfalls soll die Entscheidung über Einschluss bzw. Ausschluss von Forschungsarbeiten transparent und nach vorab definierten Kriterien erfolgen [Br09; Oa11; Go11]. In der folgenden Aktivität 4 werden die in den identifizierten Studien zu findenden Forschungsergebnisse auf ihren möglichen Beitrag zur Beantwortung der Forschungsfrage betrachtet; bspw. ob in der

betreffenden Studie Variablen und Konstrukte untersucht werden, die den der Forschungsfrage entsprechen bzw. ihnen zugeordnet werden können. Im vorletzten Schritt geht es darum, das so gesammelte Wissen – bzw. die so gesammelte Evidenz –, das einen Beitrag zur Beantwortung der Forschungsfrage leisten kann, zusammenfassend darzustellen. Dies kann mittels tabellarischer Übersichten erfolgen, es können allerdings auch statistische Verdichtungen von Forschungsergebnissen infrage kommen, wenn in den Studien entsprechende Daten veröffentlicht wurden.

Das Vorgehensmodell erscheint in der dargestellten Form zunächst recht linear, allerdings ist es gegebenenfalls empfehlenswert, Rückschritte zuzulassen, bspw. weil sich eine Forschungsfrage als zu eng oder als zu breit herausgestellt hat oder weil Kriterien für den Einschluss zu eng definiert worden sind. Entsprechend sollte dem Hinweis aus der medizinischen Reviewforschung Beachtung geschenkt werden: „these questions should not become a straitjacket that prevents exploration of unexpected issues“ [HG11]. Gleichwohl ist es erforderlich, entsprechende Anpassungen zu begründen und darüber transparent zu berichten.

Im Folgenden wird entlang dieses skizzierten Vorgehens ein systematischer Review für das Themengebiet Informationssicherheitsmanagement durchgeführt, wobei – aufgrund von Seitenrestriktionen – dieses für einen Ausschnitt vertieft wird.

3 Systematischer Review

3.1 Definition der Forschungsfrage

Der erste Schritt besteht darin, eine Forschungsfrage für den Review zu definieren. Dabei wird empfohlen, die Forschungsfrage nicht nur frei sondern auch in einer strukturierten Form zu formulieren. In der einfachsten Form besteht eine Forschungsfrage aus zwei Variablen und der Nennung von Gründen für eine (angenommene) Beziehung zwischen diesen [Co09, S. 22]. Weitere Komponenten, die zur Konkretisierung genannt werden können sind bspw. die Spezifikation des Gegenstandsbereichs und von Studienarten (Forschungsdesigns), die einbezogen werden sollen [Wh09].

Die Forschungsfrage „*Welche empirische Evidenz gibt es bezüglich der Faktoren, die die Informationssicherheit beeinflussen?*“ stellt sich in einer strukturierten Form demnach wie in Abbildung 2 angegeben dar (Nr. 1). Da die möglichen Faktoren und auch diejenigen, zu denen empirische Studien vorliegen, sehr vielfältig sind und die Forschungsfrage demnach sehr generell ist, scheint es angeraten, sie feingranularer zu formulieren (siehe oben 2.2). Hierbei kann die strukturierte Formulierung der Forschungsfrage unterstützend herangezogen werden, denn es können – wie in Abbildung 2 gezeigt – die einzelnen Komponenten der Forschungsfrage jeweils für sich einzeln spezialisiert werden.

So lassen sich bezüglich der Faktoren, die die Informationssicherheit beeinflussen „soziale Faktoren“, „eingesetzte Schutzmechanismen“ etc. unterscheiden (als unabhängige Variablen). Ebenfalls lässt sich die abhängige Variable spezialisieren, indem nicht allein

allgemein nach „Informationssicherheit“ als dem relevanten Endpunkt gefragt wird, sondern die „Einhaltung von Richtlinien (Policy Compliance)“ als ein feingranularer Aspekt der Informationssicherheit betrachtet wird. Eine mögliche, sich nach dieser Spezialisierung ergebende Forschungsfrage, die im Folgenden näher betrachtet werden soll lautet demnach (Forschungsfrage Nr. 1.1.1 in Abbildung 2):

„Welche empirische Evidenz liegt vor bezüglich sozialer Faktoren, die die Einhaltung von Richtlinien (Policy Compliance) beeinflussen?“.

Nr.	**Spezifikation des Gegenstandsbereichs**	**Untersuchte Variablen**		**Studienarten (Forschungsdesigns)**
		Unabhängige Variable	**Abhängige Variable (Endpunkt, „Outcome“)**	
1	Informationssicherheitsmanagement	Allgemein „Faktoren“	Informationssicherheit	Empirische Studien
1.1	Informationssicherheitsmanagement	Soziale Faktoren	Informationssicherheit	Empirische Studien
1.1.1	Informationssicherheitsmanagement	Soziale Faktoren	Einhaltung von Richtlinien (Policy Compliance)	Empirische Studien
1.2	Informationssicherheitsmanagement	Eingesetzte Controls (Countermeasures, Maßnahmen, Schutzmechanismen)	Einhaltung von Richtlinien (Policy Compliance)	Empirische Studien
…	…	…	…	…
…	Technische IT-Sicherheit	Firewalls	Informationssicherheit	Simulationsstudien
…	…	…	…	…

Abbildung 2: Strukturierte Definition der Forschungsfrage

In der vorletzten Zeile wird deutlich, dass mittels der strukturierten Formulierung der Forschungsfrage auch andere Aspekte als das Informationssicherheitsmanagement aufgenommen werden könnten, wenn man als Faktoren auch technische Produkte wie zum Beispiel Firewalls auffasst.

3.2 Suche nach relevanten Studien in der Primärforschung und Anwendung von Einschluss-/Ausschlusskriterien

Für die stichwortbasierte Recherche wurde die erste, generelle Forschungsfrage zugrunde gelegt (Nr 1). Die Durchführung dieser zweiten Aktivität orientiert sich an in der Literatur vorgeschlagenen Schritten (bspw. [Br09]).

Die Literatursuche erfolgte zunächst unter Verwendung der Stichwörter Information Security, IT Security, System Security und den deutschen Übersetzungen sowie unter Verwendung empirischer Forschungsmethoden (Case Study, Survey, Experiment …), da beabsichtigt ist, empirische Evidenz zur Beantwortung der Forschungsfrage heranzuziehen und zu konsolidieren. Gesucht wurde in relevanten Portalen (ABI/INFORM, EBSCO, Emerald, ScienceDirect, Springerlink). Im Ergebnis wurden 2286 Treffer er-

zielt, die nach dem Entfernen von unpassenden Studien/Arbeiten (bspw. fiktiven Fallstudien) sowie Duplikaten und der Anwendung von Ein- und Ausschlusskriterien auf 354 Studien verdichtet werden konnten. Diese Primärarbeiten wurden in einer Datenbank erfasst und stehen nun für weitere, spezifischere Auswertungen und auf diesen basierenden Reviews zur Verfügung.

Für diesen Beitrag wird ein Ausschnitt betrachtet, der diejenigen Arbeiten umfasst, die auf die Untersuchung sozialer Faktoren und die Einhaltung von Richtlinien (Policy Compliance) abzielen. Dies entspricht der in Abbildung 2 genannten Forschungsfrage Nr. 3. Hierzu liegen insgesamt lediglich 9 empirische Studien vor, die im engeren Sinne die beiden Variablen und eine (angenommene) Beziehung zwischen diesen untersuchen. An dieser Stelle des Vorgehensmodells ist eine Iteration zwischen den Aktivitäten 3 und 4 erforderlich, da erst die nähere Analyse der Ergebnisse die Erkenntnisse bringt, die die angemessene Anwendung der Ausschlusskriterien erlaubt.

3.3 Analyse der Ergebnisse der Primärforschung mit Blick auf die Forschungsfrage

In der vierten Aktivität gilt es, aus den Primärarbeiten relevante Informationen zu entnehmen, die einen Beitrag zur Beantwortung der Forschungsfrage leisten können [Go09; Co09]. Hierzu werden die untersuchten Variablen den in der Forschungsfrage definierten Variablen zugeordnet. Typischerweise sind die untersuchten Variablen und Konstrukte Spezialisierungen oder Ausprägungen der in der Forschungsfrage genannten Variablen. Bspw. werden in den von den Verfassern untersuchten Studien als sozialen Faktoren *Einstellung* (Attitude), *Wahrgenommene Verhaltenskontrolle* (Perceived Behavioral Control) und *subjektive Maßstäbe* (Subjective Norms) genannt. Diese Variablen und die in den Studien berichteten Beziehungen zu den Endpunkten werden für weitere Darstellungen und Auswertungen erfasst.

3.4 Zusammenfassung (Integration/Synthese) der Ergebnisse

Zur zusammenfassenden Darstellung der Ergebnisse existieren verschiedene Darstellungsmöglichkeiten, die auf unterschiedlichen Voraussetzungen beruhen. Unterschieden werden die qualitativ- und die quantitativ-orientierte Ergebnispräsentation. Von der Reviewforschung werden auf der einen Seite eher qualitative-tabellarische Darstellungen und auf der anderen Seite quantitativ-statistische Verdichtungen vorgeschlagen [Co09, S. 219]. Letztere erfolgen in sogenannten Metaanalysen und sind dann möglich, wenn in den Primärstudien die empirischen Daten bzw. aus ihnen errechnete statistische Kennzahlen berichtet werden.

Abbildung 3 enthält eine qualitativ-tabellarische Ergebnispräsentation, die sich an sogenannte Summary-of-Findings-Tabellen anlehnt. Eine solche Tabelle gilt in medizinischen Reviews als das Standardinstrument zur Darstellung von Ergebnissen.[1]

[1] Das bereits erwähnte Cochrane Handbook (HG11) beschreibt diese Tabellen folgendermaßen: „A ‘Summary of findings’ table provides key information concerning the quality of evidence, the magnitude of effect of the interventions examined, and the sum of available data on all important outcomes for a given comparison“

Abbildung 3: Summary-of-Findings-Tabelle zur Darstellung der Ergebnisse (Teil 1)

Studie	**Studiendesign, bereitgestellte Evidenz**	**Variablen der Forschungsfrage**		**Ergebnisse**
		Soziale Faktoren	**Endpunkt: Einhaltung von Richtlinien Policy Compliance**	
Hazari et al. [HHC08]	- Survey - Empirical, quantitative evidence	- Attitude - Subjective Norm - Behavioral Control	Behavioral Intention	- Attitude *** - Perceived Behavioral Control *** - Subjective Norm
Bulgurcu et al. [BCB10]	- Survey - Empirical, quantitative evidence	- Attitude - Normative Beliefs - Self-Efficacy	Intention to Comply	- Attitude *** - Normative Beliefs *** - Self-Efficacy ***
Johnston and Warkentin [JW10]	- Lab Experiment - Empirical, quantitative evidence	- Response Efficacy - Self-Efficacy - Social Influence	Behavioral Intent	- Response Efficacy *** - Self-Efficacy *** - Social Influence ***
Zhang et al. [ZRL09]	- Survey - Empirical, quantitative evidence	- Attitude - Subjective Norms - Perceived Behavioral Control	Intention	- Attitude *** - Subjective Norms - Perceived Behavioral Control ***
Herath and Rao [HR09a]	- Survey - Empirical, quantitative evidence	- Attitude - Punishment Severity - Detection Certainty - Subjective Norm - Descriptive Norm	Security Policy Compliance Intention	- Attitude - Punishment Severity *** - Detection Certainty *** - Subjective Norm *** - Descriptive Norm ***

Abbildung 3: Summary-of-Findings-Tabelle zur Darstellung der Ergebnisse (Teil 2)

Studie	Studiendesign, bereitgestellte Evidenz	Variablen der Forschungsfrage		Ergebnisse
		Soziale Faktoren	Endpunkt: Einhaltung von Richtlinien Policy Compliance	
Myyry et al. [MSPVV09]	- Survey - Empirical, quantitative evidence	- Preventional reasoning - Conventional reasoning - Postconventional reasoning - Openness to change - Conservation	(Hypothetical and Actual) Compliance with ISP	- Preventional reasoning *** - Conventional reasoning - Postconventional reasoning - Openness to change *** - Conservation *** (*negative correlation*)
Herath and Rao [HR09b]	- Survey - Empirical, quantitative evidence	- Severity of Penalty - Certainty of Detection - Normative Beliefs - Peer Behavior - Perceived Effectiveness	Policy Compliance Intention	- Severity of Penalty *** (*negative correlation*) - Certainty of Detection *** - Normative Beliefs *** - Peer Behavior *** - Perceived Effectiveness ***
Foltz et al. [FSA08]	- Survey - Empirical, quantitative evidence	- Attitude - Social Trust - Apathy - Subjective Norm - Perceived Behavioral Control	Behavioral Intention	- Attitude *** - Social Trust *** - Apathy *** (*negative correlation*) - Subjective Norm - Perceived Behavioral Control
Pahnila et al. [PSM07]	- Survey - Empirical, quantitative evidence	- Intention to comply - Information quality - Rewards	Actual compliance	- Intention to comply *** - Information quality *** - Rewards

Die hier dargestellte und angepasst Summary-of-Findings-Tabelle orientiert sich an in den Forschungsfrage genannten Variablen, nennt darüber hinaus pro Studie das Studiendesign (die Forschungsmethode der Primärarbeit), charakterisiert die bereitgestellte Evidenz (hier nur empirische Evidenz) und beschreibt in der letzten Spalte die Ergebnisse der Studien mit Blick auf die relevanten Variablen. Da sämtliche identifizierte empirische Studien in englischer Sprache verfasst sind, haben sich die Verfasser entschieden, auch die Variablen jeweils im Original zu zitieren.

3.5 Diskussion

Die Summary-of-Findings-Tabelle enthält die sozialen Faktoren, die bisher in der Literatur mit Blick auf die Einhaltung von Richtlinien (Policy Compliance) untersucht worden sind bzw. genauer gesagt diejenigen, die mittels der durchgeführten Literatursuche (Aktivität 2) gefunden werden konnten.

Nr.	Variable	Vermutete Korrelation	Studien mit signifikanten Ergebnissen / Gesamtzahl Studien
1	Attitude	Positiv	4 / 5
2	Subjective Norm	Positiv	1 / 4
3	Perceived Behavioral Control	Positiv	2 / 3
4	Certainty of Detection	Positiv	2 / 2
5	Normative Beliefs	Positiv	2 / 2
6	Self-Efficacy	Positiv	2 / 2
7	Apathy	Positiv	1 / 1
8	Conservation	Negativ	1 / 1
9	Conventional reasoning	Positiv	0 / 1
10	Descriptive Norm	Positiv	1 / 1
11	Information quality	Positiv	1 / 1
12	Intention to comply	Positiv	1 / 1
13	Openness to change	Positiv	1 / 1
14	Peer Behavior	Positiv	1 / 1
15	Perceived Effectiveness	Positiv	1 / 1
16	Postconventional reasoning	Positiv	0 / 1
17	Preventional reasoning	Positiv	1 / 1
18	Punishment severity	Positiv	1 / 1
19	Response Efficacy	Positiv	1 / 1
20	Rewards	Positiv	0 / 1
21	Severity of Penalty	Negativ	1 / 1
22	Social Influence	Positiv	1 / 1
23	Social Trust	Positiv	1 / 1

Abbildung 4: Variablen, die als Soziale Faktoren in Bezug auf Einhaltung von Richtlinien (Policy Compliance) untersucht wurden

Insgesamt wurden 23 verschiedene Variablen identifiziert, wovon für 20 Variablen empirische Evidenz für eine Korrelation vorliegt. Abbildung 4 listet die Variablen in absteigender Reihenfolge nach Anzahl der Studien, in denen sie untersucht wurden, auf. Sechs Variablen wurden in mehreren Primärstudien untersucht. Forscher im Gebiet der Informationssicherheitsmanagement-Forschung können diese Darstellung und die Summary-of-Findings-Tabelle nutzen, um relevante Studien zu identifizieren oder aber auch um Variablen zu identifizieren, die ihrer Ansicht nach oder gemäß einschlägiger Theorien als relevant anzusehen sind, bisher aber keine Beachtung in der Literatur gefunden haben. In diesem Sinne dient die Analyse dem Auffinden von Forschungslücken [Go09; Co09].

Betrachtet man die hier untersuchten Variablen und Faktoren und dabei insbesondere diejenigen, die mehrfach untersucht wurden, so lässt sich eine deutliche Dominanz der "theory of planned behavior" (TPB) als theoretische Basis in diesem Bereich erkennen. Für zukünftige Forschungsarbeiten der Informationssicherheitsmanagement-Forschung könnte sich die Heranziehung alternativer Theorien anbieten, um die theoretische Basis zu verbreitern, insbesondere da nicht alle Faktoren der TPB eine hohe Evidenz aufweisen.

So zeigt ein Blick in die Summary-of-Findings-Tabelle, dass für die Variable „Attitude" in vier Studien positiv signifikante Ergebnisse vorliegen und lediglich in der Studie von Herath und Rao [HR09a] ein nicht-signifikantes positives Ergebnis gemessen wurde. Durch die gemeinsame Betrachtung der fünf Studien kann man daher nach Ansicht der Verfasser auf eine „harte Evidenz" und damit auf eine gute Evidenzlage bezüglich dieser Variable und ihrer positiven Korrelation schließen.

Ein ähnliches Bild ergibt sich bei der Variable *wahrgenommene Verhaltenskontrolle* (Perceived Behavioral Control). Hier liefern zwei Studien signifikant positive Ergebnisse und bestätigen damit eine positive Korrelation zur *Einhaltung von Richtlinien* (Policy Compliance). Die Studie von Foltz et al. [FSA08] stellt hierzu eine gewisse Relativierung dar, da sie keine Bestätigung für einen positiven Zusammenhang bietet.

Bei einer dritten Variable, den *subjektiven Maßstäben* (Subjective Norms), hingegen ergibt die Gesamtschau, dass es keine empirische Evidenz für einen positiven Effekt gibt. Im Gegenteil, empirische Evidenz liegt dafür vor, dass wahrscheinlich kein positiver Zusammenhang angenommen werden kann: Nur in [HR09a] ist ein signifikant positiver Effekt erkennbar; in drei weiteren Untersuchungen wird diese Variable zwar betrachtet, allerdings kann eine Korrelation nicht bestätigt werden.

Anhand der Ergebnisse zu den genannten Variablen, allesamt aus der TPB entnommen, lässt sich der „fit" der TPB für Fragestellungen der ISP Compliance zumindest in Frage stellen. Womöglich ist eine adaptiere TPB vonnöten, was weitere Forschung bzgl. der theoretischen Basis erfordert.

Insgesamt ist insbesondere die Analyse und Diskussion von Variablen, die mehrfach in Studien untersucht wurden, ein fruchtbares Unterfangen. So können aus

unterschiedlichen und konfligierenden Ergebnissen möglicherweise weitere Erkenntnisse gewonnen, bestehende Annahmen kritisch reflektiert, und die Wissensbasis gestärkt werden.

4 Fazit und weiterer Forschungsbedarf

Ziel des Beitrags war es zu zeigen, wie die Kumulierung empirischer Forschungsergebnisse in der Informationssicherheitsmanagement-Forschung erfolgen kann und welcher Nutzen sich hieraus ergibt. Zu diesem Zweck wurde ein Vorgehensmodell zur Anfertigung systematischer Reviews präsentiert und es wurden die grundlegenden Schritte bei der Durchführung eines konkreten Reviews skizziert.

Erste konkrete Ergebnisse konnte bezüglich sozialer Faktoren präsentiert werden. Dabei wurden 23 soziale Faktoren als Variablen identifiziert, die ein spezifisches Ziel des Informationssicherheitsmanagements, nämlich die Einhaltung von Richtlinien, beeinflussen. Im Ergebnis wurde dargelegt, welche empirische Evidenz für ihren Einfluss im Sinne von wissenschaftlichen Belegen oder wissenschaftlichem Nachweis vorliegen. Für fünf Studien kann so eine verbesserte Evidenzlage, die über die Ergebnisse von Einzelstudien hinausgeht, konstatiert werden.

Dieser Review erlaubt Forschern im Gebiet des Informationssicherheitsmanagements Forschungslücken zu identifizieren – bspw. mit Blick auf fehlende empirische Evidenz zu einschlägigen Faktoren – und Anregungen für die theoretische Basis und die Notwendigkeit ihrer Erweiterung abzuleiten.

Die Ergebnisse können darüber hinaus Praktikern oder gestaltungsorientierten Forschern, die ihrer Arbeit auf wissenschaftliche empirische Evidenz stützen wollen, eine gewisse Hilfestellung geben. So lässt sich aus den kumulierten Ergebnissen schließen, dass die *Einstellung/Haltung* (Attitude) der Benutzer in wissenschaftlichen Studien als ein wichtiger Einflussfaktor auf die Informationssicherheit erkannt wurde, ebenso wie die w*ahrgenommene Verhaltenskontrolle* (Perceived Behavioral Control) und auch *normative Überzeugungen/Einstellungen* (Normative Beliefs) und *Selbstwirksamkeit(serwartung)* (Self-Efficacy). Hingegen ist die Evidenzlage bezüglich *subjektiver Maßstäbe* (Subjective Norms) unklar bis eher negativ.

Diese Ergebnisse lassen sich zwar nicht unmittelbar in IT-Artefakte übersetzen, allerdings scheinen sie geeignet, Designentscheidungen zu begründen und auf diese Art und Weise – im Sinne von [FHL10], [Ge09] und [PMG11] – theoretische Erkenntnisse und empirisches Wissen für Design-Science-Forschung und die Entwicklung von Konzepten und Methoden für das Informationssicherheitsmanagement nutzbar zu machen. So könnte man die Größen, die den hier betrachteten Faktoren zugrunde liegen, näher mit Blick darauf analysieren, ob sie sich durch Maßnahmen manipulieren lassen und sie somit dem Management zugänglich sind. Gleichwohl ist die Übertragung empirischer Forschungsergebnisse in die Design-Science-Forschung gewiss eine Aufgabe, für die erst noch ein stabiles forschungsmethodisches Fundament entwickelt werden muss.

Bedarf zur Weiterentwicklung und weiterer Forschung sehen die Verfasser darüber hinaus in methodischer und inhaltlicher Hinsicht.

Eine methodische Verbesserung könnte auf die Ergebnisdarstellung zielen. Bislang liegt nur eine Summary-of-Findings-Tabelle vor, die bei einer größeren Anzahl von Studien schwer handhabbar werden dürfte; an dieser Stelle wäre zu prüfen, ob graphenbasierte oder andere grafische Darstellungen die Präsentation und damit auch die Kommunikation der Ergebnisse zweckmäßig unterstützen können.

Darüber hinaus sollten in weiteren Studien mittels Metaanalysen die hier verbal diskutierten Ergebnisse statistisch verdichtet und analysiert werden und es bietet sich an, die Heterogenität, die sich aus unterschiedlichen Populationen und Studiendesigns ergeben kann, näher zu analysieren [Co09].

Des Weiteren gilt es, neben der empirischen Evidenz andere Evidenzarten einzubeziehen, da bspw. bei technischen Fragen in der Informationssicherheit häufig simulationsbasierte Evaluationsverfahren angewendet werden, um die Vorteilhaftigkeit von Artefakten und Produkten zu untersuchen [bspw. Mi10].

Zusätzlich sind inhaltliche Erweiterungen erforderlich. An dieser Stelle wurden nur für einen kleinen Ausschnitt des Forschungsfeldes, der aus der übergeordneten Forschungsfrage abgeleitet werden konnte, konkrete Ergebnisse präsentiert. Die strukturierte Formulierung der Forschungsfrage erlaubt dabei, das Forschungsfeld zu systematisieren. Um in diesem Schritt konsistent zur vorhandenen Literatur zu sein, bietet es sich an, in späteren Forschungsarbeiten bereits vorhandene Informationssicherheits-Ontologien zu nutzen [bspw. Bl08; MG10].

Darüber hinaus ist ein weiteres Ziel – aufbauend auf den bereits erfassten Studien (siehe 3.2) –, konkrete inhaltliche Ergebnisse für andere spezifische Forschungsfragen und schlussendlich auch für die übergeordnete Forschungsfrage, „*Welche empirische Evidenz gibt es bezüglich der Faktoren, die die Informationssicherheit beeinflussen?*“, herauszuarbeiten. Insbesondere dann, wenn die Nutzung empirischer Ergebnisse für die Design-Science-Forschung auch methodisch besser durchdrungen ist, könnten auf dieser Grundlage Methoden und Konzepte für die Informationssicherheit entwickelt bzw. weiterentwickelt werden.

Literaturverzeichnis

[BCB10] Bulgurcu, B.; Cavusoglu, H.; Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, (34:3), 2010, S. 523-A7.

[Bl08] Blanco, C., Lasheras, J., Valencia-Garcia, R., Fernandez-Medina, E., Toval, A. and Piattini, M. (2008) A Systematic Review and Comparison of Security Ontologies, Proc. of the Third International Conference on Availability, Reliability and Security, 813-819.

[Br09] vom Brocke, J.; Simons, A.; Niehaves, B.; Riemer, K.; Plattfaut, R.; Cleven, A.: Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search

Process. Proceedings of the 17th European Conference on Information Systems (ECIS), 2009, S. 2206-2217.
[BZ03] Benbasat, I.; Zmud, R.W.: The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties. MIS Quarterly, (27:2), 2003, S. 183-194.
[Ca11] Card, N.A.: Applied meta-analysis for social science research. Guilford Press, 2011.
[Co09] Cooper, H.: Research Synthesis and Meta-Analysis. Sage, London, 2009.
[FHL10] Fettke, P., Houy, C., Loos, P.: On the Relevance of Design Knowledge for Design-Oriented Business and Information Systems Engineering. Business & Information Systems Engineering 2 (6), 347–358.
[FSA08] Foltz, C.B.; Schwager, P.H.; Anderson, J.E.: Why users (fail to) read computer usage policies. Industrial Management & Data Systems, (108:6), 2008, S. 701-712.
[Ge09] Gehlert, A.; Schermann, M.; Pohl, K.; Krcmar, H.: Towards a Research Method for Theory-Driven Design Research. Hansen, H. R,; Karagiannis, D.; Fill, H.-G. (Hrsg.) Proceedings der 9. Intl.en Tagung Wirtschaftsinformatik - Business Services: Konzepte, Technologien, Anwendungen, 25.-27. Februar 2009, Wien, Österreich. 2009, S. 441-450
[Go09] Gough, D.: Qualitative, quantitative and mixed methods systematic reviews to support professional decision making in education. In (Böttcher, W.; Dicke, J.N.; Ziegler, H., Hrsg.): Evidenzbasierte Bildung Wirkungsevaluation in Bildungspolitik und pädagogischer Praxis. Waxmann Verlag, Münster, 2009, S. 23-33.
[Go11] Goeken, M.: Towards an Evidence-based Research Approach in Information Systems, ICIS 2011 Proceedings. Paper 10, 2011. http://aisel.aisnet.org/icis2011/proceedings/researchmethods/10
[HG11] Higgins, J.P.T.; Green, S.: Cochrane Handbook for Systematic Reviews of Interventions. Version 5.1.0, 2011. http://www.cochrane-handbook.org/
[HHC08] Hazari, S.; Hargrave, W.; Clenney, B.: An Empirical Investigation of Factors Influencing Information Security Behavior. Journal of Information Privacy & Security, 4(4), 2008, S. 3-20.
[HR09a] Herath, T.; Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18, 2009, S. 106-125.
[HR09b] Herath, T.; Rao, H.R.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47, S. 154-165.
[Ki09] Kitchenham B.A., Brereton O.P., Budgen D., Turner M., Bailey J., Linkman S.: Systematic literature reviews in software engineering – a systematic literature review. Information and Software Technology, 51, S. 7-15.
[JW10] Johnston, A. C.; Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, (34:3), 2010, S. 549-A4.
[MG10] Milicevic, D.; Goeken, M.: Ontology-based Evaluation of ISO 27001. Software Services for e-World - 10th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2010, Buenos Aires, Argentina, November 3-5, 2010. Proceedings; 01/2010
[Mi10] Miede, A.: Cross-organizational Service Security – Attack Modeling and Evaluation of Selected Countermeasures. Verlag Dr. Hut, München 2010.
[MS07] Markus, M.L.; Saunders, C.S.: Looking for a Few Good Concepts … and Theories … for the Information Systems Field. MIS Quarterly, (31:1), 2007, S. iii-vi.
[MSPVV09] Myyry, L.; Siponen, M.; Pahnila, S.; Vartiainen, T.; Vance, A.: What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18, 2009, S. 126-139.
[Oa11] Oates, B.: Evidence-based Information Systems: A Decade Later. ECIS 2011 Proceedings, 2011, Paper 222. http://aisel.aisnet.org/ecis2011/

[PMG11] Patas, J.; Milicevic, D.; Goeken, M.: Enhancing design science through empirical knowledge: framework and application. Proceedings of the 6th international conference DESRIST'11. Springer, Berlin, S. 32-46.

[PSM07] Pahnila, S.; Siponen, M.; Mahmood, A.: Employees' Behavior towards IS Security Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences, 2007, S. 156-166.

[Sa11] Sackmann, S.: IT-Sicherheit. Kurbel, K.; Becker, J.; Gronau, N.; Sinz, E.;Suhl, L. (Hrsg.): Enzyklopädie der Wirtschaftsinformatik, Online-Lexikon, Oldenbourg-Verlag, München, 2008. www.enzyklopaedie-der-wirtschaftsinformatik.de

[SWB08] Siponen, M.; Willison, R.; Baskerville, R.: Power and Practice in Information Systems Security Research. ICIS 2008 Proceedings. 2008, Paper 26.

[VRG02] Vessey, I.; Ramesh, V.; Glass, R.L.: Research in information systems: an empirical study of diversity in the discipline and its journals. Journal of Management Information Systems (19:2), 2002, S. 129-174.

[Wh09] White, P.: Defining a research question. In (Verhagen, E.; Mechelen, W.V., Hrsg.): Sports Injury Research, Oxford University Press, 2009, S. 3-9.

[WW02] Webster, J.; Watson, R.T.: Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, (26:2), 2002, S. xiii – xxiii.

[ZRL09] Zhang, J.; Reithel, B.J.; Li, H.: Impact of perceived technical protection on security behaviors. Information Management & Computer Security, (17:4), 2009, S. 330-340.