Informationssicherheit und Persönlichkeit : Konzept, Empirie und Handlungsempfehlungen

Der Wirtschaftswissenschaftlichen Fakultät der

Gottfried Wilhelm Leibniz Universität Hannover

zur Erlangung des akademischen Grades

Doktor der Wirtschaftswissenschaften

- Doctor rerum politicarum -

vorgelegte Dissertation

von

Diplom-Ökonom Robert André Pomes

geboren am 30.01.1975 in Salzgitter

2011

Inhaltsverzeichnis

„Alles Wissen und alles Vermehren unseres Wissens endet nicht
mit einem Schlußpunkt, sondern mit einem Fragezeichen.“
(Hermann Hesse)

Executive Summary

PIETSCH, HEINRICH und BIZER zeigen unmissverständlich auf, dass in heutigen Informationsgesellschaften zum einen Geschäftsprozesse unteilbar mit Informations- und Kommunikationsprozessen verbunden sind und zum anderen die Bedeutung von wissensintensiven Produkten und Dienstleistungen zunehmend steigt. Demgemäß entscheiden positive werthaltige wie negative und damit schädigende Informationen schließlich über den Erfolg und die Wettbewerbsfähigkeit einer Organisation und sind zu schützen. Die Sicherheit von Informationssystemen wird nach den Ausführungen von BASKERVILLE und JAEGER daher zunehmend systemrelevant und sollte als Ernst zunehmendes Thema eingestuft werden, insbesondere weil Schwachstellen und Gefahren in der digitalen Welt permanent steigen. Die Gewährleistung der Informationssicherheit wird hiernach zu einer Schlüsselaufgabe, welche den Fortbestand der Organisation bedingen kann. Demgemäß ist die technische Absicherung der Informationen unbedingt notwendig, jedoch zeigt sich nach KRUGER und KEARNEY eine breite Akzeptanz dafür, dass „…involvement of humans in information security is equally important and many examples exist where human activity can be linked to security issues“, womit der Mensch in den Mittelpunkt des Interesses rückt. Diesen führen auch GONZALES, HUANG und HOONAKKER übereinstimmend in ihren aktuellen Forschungen zur Erhöhung der Informationssicherheit auf und VENEABLES bezeichnete die menschliche Schwachstelle als „…the most difficult to manage because you cannot control what is in people‘s heads and what they will be willing to talk about inadvertently or otherwise“. Dementsprechend ist die Sicherheit von Informationssystemen nicht allein durch technische Maßnahmen zu gewährleisten, sondern es bedarf vielmehr der Notwendigkeit der gesamthaften Betrachtung der Technologie, des Menschen und der Prozesse wie bspw. SPEARS, DONTAMSETTI und NARAYANAN anführen. Das Interesse der vorliegenden Arbeit richtet sich hierbei auf die Fragestellung, welche Zusammenhänge zwischen Menschen und technischen, rechtlichen, organisatorischen sowie wirtschaftlichen Aspekten einer Organisation bestehen und inwieweit dadurch die Sicherheit von Informationen erhöht respektive reduziert wird.

Im Rahmen dieser Arbeit wurden die Zusammenhänge zwischen der menschlichen Persönlichkeit von IT-Entscheidern und der Sicherheit von Informationssystemen, veranlasst durch mehrere Gründe, erforscht: (1) Der Mensch stellt nachweislich das größte Risiko bei der Gewährleistung der Sicherheit von Informationen dar. (2) Die Beschreibung des Verhaltens von Organisationsmitgliedern durch Methoden der differentiellen Psychologie und der Persönlichkeitsforschung haben eine hohe Aktualität. (3) Zusammenhänge zwischen der menschlichen Persönlichkeit und der Sicherheit von Informa-

tionen werden im günstigen Fall rudimentär behandelt. Das Anliegen der vorliegenden Arbeit besteht darin, die bestehende Forschungslücke durch eine empirische Untersuchung weiter zu schließen.

Als Ausgangspunkt für diese Untersuchung waren folgende Forschungsfragen handlungsleitend:

1. ***Welche Zusammenhänge existieren zwischen der Informationssicherheit und den Persönlichkeitsmerkmalen von IT-Entscheidern?***
2. ***Welche Handlungsempfehlungen können, bei Berücksichtigung der Persönlichkeitsmerkmale von IT-Entscheidern, zur Erhöhung der Informationssicherheit identifiziert werden?***

Die Forschungsfragen bedurften der weiteren Operationalisierung sowie der Ausgestaltung eines konzeptionellen Bezugsrahmens, welcher den Forschungsbereich der Informationssicherheit durch die technische, rechtliche, organisatorische und wirtschaftliche Dimension darstellt. Durch diesen Bezugsrahmen wurden die wesentlichen Einflussfaktoren auf die Ebene der Prozesse, der Technik sowie des Menschen ermittelt. Es wurden adäquate Fragestellungen sowie geeignete Antwortoptionen operationalisiert. Die Erfassung der menschlichen Persönlichkeit wurde durch Theorien zur Persönlichkeit vorgenommen, welche hypothetische Aussagen über ihre Struktur und Funktionsweise lieferten. Diese Aussagen wurden auf der einen Seite genutzt, um Erkenntnisse über den Aufbau, die Struktur und die Zusammenhänge der Persönlichkeit zu generieren. Auf der anderen Seite wurden, basierend auf dem Wissen über die Persönlichkeit, Vorhersagen über Verhaltensweisen getroffen, welche zu eindeutigen Handlungsempfehlungen führten. Dabei bilden die Vorhersagen über Verhaltensweisen die Grundlage, Menschen so zu sensibilisieren, dass sie mit gegenwärtigen, neuartigen und komplexen Gefahren für die Informationssicherheit zurechtkommen. Die Erfassung der menschlichen Persönlichkeit erfolgte, aufgrund der hohen Güte und des standardisierten Messinstruments, über das NEO-FFI-Modell, welches die Persönlichkeit über den Trait-Ansatz feststellt und im deutschsprachigen Raum von BORKENAU und OSTENDORF geprägt wurde. In dieser Taxonomie wurde die menschliche Persönlichkeit durch die fünf Persönlichkeitsmerkmale Neurotizismus, Extraversion, Offenheit für Erfahrung, Verträglichkeit und Gewissenhaftigkeit beschrieben, welche in den letzten Jahrzehnten wegweisend durch GOLDBERG, MCCRAE und JOHN geformt wurden.

Aufbauend auf die konzeptionellen Vorüberlegungen, wurde ein Fragebogen mit den Teilbereichen Persönlichkeit, Informationssicherheit und Soziodemographie entwickelt, welcher die Grundlage zur Durchführung der empirischen Untersuchung bildete. Die Analyse der erhobenen Daten erfolgte durch Methoden der induktiven Statistik, wie Regressions- und Korrelationsanalysen. Die gewonnenen Daten wurden anhand von Gütekriterien wie Objektivität, Validität und Reliabilität verifiziert oder falsifiziert und deskriptiv dargestellt. Nachfolgende Abbildung stellt die beschriebene Vorgehensweise der vorliegenden Arbeit dar:

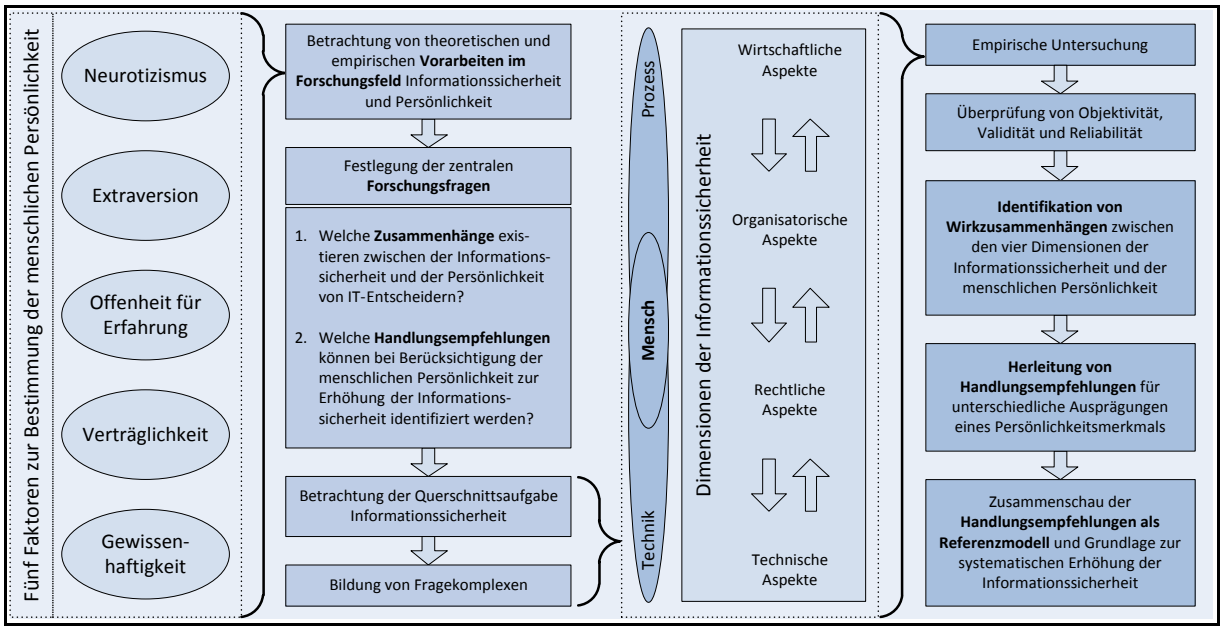

Abbildung 2: Vorgehensweise der vorliegenden Arbeit
Quelle: Eigene Darstellung

Durch die Analyse der erhobenen Daten, mittels Methoden der induktiven Statistik, wurden Wirkzusammenhänge identifiziert sowie Handlungsempfehlungen wissenschaftlich stringent erarbeitet. Zur systematischen Reduzierung des festgestellten Erkenntnisdefizites wurden vorab dargestellte grundlegende Forschungsfragen durch detailliertere Fragen weiter ausdifferenziert, welche im Folgenden beantwortet werden. Eine Detailfrage ersuchte die Relevanz zu klären, welche dem Menschen zur Gewährleistung der Informationssicherheit in der Organisation zukommt. Der Autor kam zu dem Schluss, dass nicht nur nach der vorherrschenden Fachmeinung von einer hohen Relevanz des Faktors Mensch zur Gewährleistung der Informationssicherheit auszugehen ist, sondern erfährt auch durch die vorliegende Untersuchung Bestätigung. Hiernach äußerten befragte IT-Entscheider, im Rahmen der empirischen Untersuchung, u. a. auf die Frage nach Gefahrenbereichen, dass „Nachlässigkeit und Irrtum der eigenen Mitarbeiter“ bei 77,2% der befragten Organisationen in der Vergangenheit für Sicherheitsvorfälle verantwortlich waren. Demnach ist der Faktor Mensch, auch im Rahmen dieser Untersuchung, der relevanteste Aspekt in diesem Sinne.

Zudem sollte geklärt werden, inwieweit ein Zusammenhang zwischen den Persönlichkeitsmerkmalen eines IT-Entscheiders und seinen Entscheidungen respektive seiner Entwicklung im organisationalen Kontext existiert. Die empirische Untersuchung ergab 62 signifikante, lineare Zusammenhänge zwischen den Fragen zur Informationssicherheit und den festgestellten Ausprägungen der Persönlichkeit. Damit bestätigt sich, dass signifikante Zusammenhänge zwischen den Ausprägungen von Persönlichkeitsmerkmalen eines Menschen und seinen Entscheidungen respektive seiner Entwicklung im organisationalen Kontext bestehen.

Mit einer weiteren Detailfrage ermittelte der Autor, welche Wirkzusammenhänge für unterschiedliche Persönlichkeitsausprägungen zu den Dimensionen der Informationssicherheit aufgezeigt werden können. Zudem wurde geklärt, welche Persönlichkeitsmerkmale einen starken und welche einen geringen Einfluss ausüben. Zu den Dimensionen der Informationssicherheit können insgesamt 62 lineare Zusammenhänge aufgeführt werden. Davon entfallen 11 auf die technische und wirtschaftliche, 10 auf die rechtliche sowie 30 - und damit fast die Hälfte - der signifikanten, linearen Zusammenhänge auf die organisatorische Dimension der Informationssicherheit. Das Persönlichkeitsmerkmal der Gewissenhaftigkeit übt mit 20 linearen Zusammenhängen den stärksten Einfluss auf das Sicherheitsverhalten von IT-Entscheidern aus und die Persönlichkeitsmerkmale der Extraversion und Verträglichkeit mit neun linearen Zusammenhängen den geringsten.

Inwiefern Vorhersagen über Entscheidungen von IT-Mitarbeitern bei unterschiedlichen Ausprägungen der Persönlichkeitsmerkmale getroffen werden können wurde im Rahmen der Arbeit beantwortet. Dazu wurden die herausgearbeiteten Wirkzusammenhänge aus den vier Dimensionen der Informationssicherheit auf ihre besondere Betonung und jeweilige Ausprägung des Persönlichkeitsmerkmals hin fortgeführt. Entsprechende Wirkzusammenhänge werden in Abschnitt 7.2 in den Tabellen 42, 44, 46, 49 und 52 dargestellt. Hierdurch lässt sich direkt vorhersagen, dass bspw. ein IT-Entscheider mit hoher Gewissenhaftigkeit annimmt, dass IT-Benutzer im Bereich der Informationssicherheit besonders geschult sind. Bei diesem Zusammenhang handelt es sich um eine signifikante Korrelation, mit einer Irrtumswahrscheinlichkeit von unter 0,1% ($\alpha<=,001$). Die berechneten Vorhersagen werden in den Tabellen 54-63 dargestellt.

Forschungsfrage 2 führt zur Quintessenz der vorliegenden Arbeit und bestimmt, welche Handlungsempfehlungen aufgrund unterschiedlicher Ausprägungen der Persönlichkeitsmerkmale für IT-Entscheider hergeleitet werden können. Im Rahmen dieser Forschungsfrage wurden die in den Wirkzusammenhängen festgestellten besonderen Betonungen zu allgemeingültigen Handlungsempfehlungen hin entwickelt. Zur Einhaltung einer wissenschaftlich widerspruchsfreien Vorgehensweise, wurde zum einen auf den konzeptionellen und inhaltlichen Orientierungsrahmen zur Informationssicherheit aus Kapitel 3 Bezug genommen, um den linearen Zusammenhang angemessen zu interpretieren. Zum anderen konnte die angemessene Interpretation der jeweiligen Ausprägung des Persönlichkeitsmerkmals nur über adäquate Eigenschaftswörter stattfinden, welche aus Tabelle 15 aus Abschnitt 4.3.2.2 herangezogen wurden. Durch diese inhaltliche Verknüpfung resultiert, bspw. aus einem linearen Zusammenhang, welcher sich in Form von einer Überbetonung von ‚Virtual Private Networks' bei Probanden mit geringem Neurotizismus ergab, die Handlungsempfehlung „Überprüfung der tatsächlichen, technischen Absicherung von Informationen bei Vorschlägen und Projekten von IT-Entscheidern". Die Grundlage hierfür bildeten zwei Aspekte: (1) ‚Virtual Private Networks' sind ein Baustein zur technischen Absicherung und ein (2) geringer Neurotizismus lässt sich u.a. durch die

Eigenschaftswörter ‚sorglos' und ‚gelassen' beschreiben. Diese Handlungsempfehlungen wurden für alle 62 erarbeiteten linearen Zusammenhänge aus Abschnitt 7.2 hergeleitet, wobei 16 Korrelationen, bei denen aufgrund der jeweiligen Antwortalternative die Fallzahl unter einem Wert von 20 lag, nur hilfsweise mit einbezogen wurden, womit sich schließlich 44 valide Handlungsempfehlungen ergaben.

Nachfolgende Tabelle zeigt die erarbeiteten Handlungsempfehlungen für die Persönlichkeitsmerkmale Neurotizismus, Extraversion, Offenheit für Erfahrung, Verträglichkeit und Gewissenhaftigkeit bei deren jeweilig geringer oder hoher Merkmalsausprägung:

Merkmal	Geringe Merkmalsausprägung	Hohe Merkmalsausprägung
Neurotizismus	• Überprüfung der tatsächlichen technischen Absicherung von Informationen bei Vorschlägen und Projekten von IT-Entscheidern • Überprüfung von Nachlässigkeit und Irrtum organisatorischer Vorschläge und Projekte von IT-Entscheidern • Überprüfung des Arbeitsklimas zwischen Mitarbeitern und IT-Entscheidern • Überprüfung, inwieweit IT-Entscheider zu sehr auf operative Maßnahmen und Pläne fixiert sind (Stichwort: Kostenrisiko und Bürokratisierung) • Begutachtung durch objektiven Dritten, inwieweit Konzepte und Richtlinien adäquat und regelmäßig überprüft werden • IT-Entscheider entsprechend entwickeln, dass sie sich selbst „mehr" mit Informationssicherheitsrisiken beschäftigen • Überprüfung der Budgetgrenzen	• Vorschläge und Entscheidungen bezüglich möglicher Gefahrenbereiche kritisch betrachten und evtl. von objektiven Dritten überprüfen lassen (Stichwort: Kostenrisiko) • Kritische Betrachtung von Vorschlägen und Entscheidungen zur Regelmäßigkeit von Konzept- und Richtlinienüberprüfungen (Stichwort: Bürokratisierung) • Überprüfung respektive Implementation von Transparenzkriterien bei Sicherheitsvorfällen • Kritische Überprüfung von erhöhten Budgetforderungen zur Verbesserung der Informationssicherheit
Extraversion	• Überprüfung der Sinnhaftigkeit und Nutzbarkeit technischer Vorschläge und Entscheidungen	• Überprüfung, inwieweit ein Ziel wie Revisionsfähigkeit zur Erhöhung der Informationssicherheit beiträgt • Überprüfung von disziplinarischen Entscheidungen gegenüber Mitarbeitern • Vorschläge und Entscheidungen bezüglich aktueller Standards und Normen sollten, im Hinblick auf ihre Relevanz, zur Erhöhung der Informationssicherheit überprüft werden • Überprüfung der Objektivität bei der Identifizierung von Sicherheitslücken • Überprüfung, inwieweit operative Konzepte die Nutzbarkeit von Informationssystemen verringern • Kritische Betrachtung von Aussagen der IT-Entscheider über die Managementebene • Kritische Betrachtung von Aussagen der IT-Entscheider über den einfachen Mitarbeiter
Offenheit für Erfahrung	• Überprüfung, inwieweit die Unternehmenskultur mit den Vorschlägen und Entscheidungen der IT-Entscheider übereinstimmt • Überprüfung, inwieweit nötige und mögliche	• Kritische Prüfung von Vorschlägen und Projekten bezüglich zukünftig notwendiger Bausteine des IS-Managements • Hinweis auf die besondere Sensibilität von

	Weiterbildungsmaßnahmen für Mitarbeiter forciert werden • Überprüfung, in welchem Umfang IT-Manager/-Abteilungsleiter in Schulungsmaßnahmen eingebunden werden	Informationen • Besondere Beachtung von Hinweisen auf Fehler von Externen • Besondere Beachtung und kritische Überprüfung von Budgetvorschlägen • Kritische Begutachtung von Äußerungen dieser Personengruppe zum empfundenen Sicherheitsniveau
Verträglichkeit	• Überprüfung der Relevanz und Adäquanz von Firewalls als Baustein des IS-Managements • Überprüfung, inwieweit bei Sicherheitsvorfällen das eigene Verhalten der IT-Entscheider ausreichend reflektiert und hinterfragt wird	• Überprüfung, inwieweit Vorschläge zu rechtlichen Aspekten aus rationalen Gründen erfolgen oder aus Gründen der Einfachheit, um einer externen Forderungen zu genügen • Besondere Beachtung und Prüfung von Sicherheitsbedenken dieser Personengruppe • Besondere Beachtung von Aussagen zu Konsequenzen von Sicherheitsvorfällen
Gewissenhaftigkeit	• Vorschläge und Projekte, welche sich den softwareseitigen Mängeln und Defekten zuwenden, sollten höchst kritisch auf ihre Notwendigkeit überprüft werden • Überprüfung, inwieweit Konzepte und Richtlinien zur Gewährleistung der Informationssicherheit regelmäßig geprüft werden • Überprüfung, inwieweit Konzepte zur Fortentwicklung der Informationssicherheit genutzt und entwickelt werden • Kritische Überprüfung von erhöhten Budgetvorstellungen	• Besondere Beachtung von Vorschlägen und Projekten zu notwendigen Bausteinen des IS-Managements • Kritische Prüfung von Vorschlägen und Projekten zu notwendigen Bausteinen des IS-Managements durch objektiven Dritten • Besondere Beachtung von Empfehlungen zu Standards und Normen • Kritische Überprüfung, inwieweit der Mehraufwand für die Ermittlung von Sicherheitslücken den Nutzen erhöht • Kritische Überprüfung von Aussagen, welcher Ebene Informationssicherheit besonders wichtig ist. • Besondere Beachtung von Empfehlungen dieser Personengruppe zu notwendigen Weiterbildungsmaßnahmen • Überprüfung, inwieweit die Schulung bestimmter Mitarbeitergruppen zur Erhöhung der Informationssicherheit beiträgt • Besondere Beachtung von Empfehlungen zum Budget für die Verbesserung der Informationssicherheit

Tabelle 63: Zusammenschau der 44 Handlungsempfehlungen
Quelle: Herleitung aus Abschnitt 7.3

Abschließend kann festgehalten werden, dass im Rahmen der vorliegenden Arbeit lineare Zusammenhänge festgestellt worden sind, womit das Entscheidungsverhalten eines IT-Mitarbeiters in den spezifischen Ausprägungen seiner Persönlichkeit erklärbar wird. Aus den identifizierten, linearen Zusammenhängen wurden Handlungsempfehlungen hergeleitet, welche als Grundlage für die Einschätzung und Entwicklung von IT-Entscheidern mit gleicher Persönlichkeitsausprägung dienen und somit zur Erhöhung der Informationssicherheit in Organisationen beitragen können. Die Zusammenschau der Handlungsempfehlungen ermöglicht es, nach Messung der Persönlichkeitsmerkmale eines IT-Entscheiders, diesbezüglich konkrete Empfehlungen zu geben.