# Einhaltung von Informationssicherheitsvorschriften durch MitarbeiterInnen: Faktoren und Maßnahmen

Barbara Krumay[1], Stefan Koch[1], und Marlene Winkler[1]

[1] Johannes Kepler Universität Linz, Österreich
{barbara.krumay,stefan.koch}@jku.at, marlenee@hotmail.de

**Abstract.** Informationssicherheitsvorschriften sind für alle Unternehmen ein wichtiges Instrument, um sich vor Sicherheitsvorfällen zu schützen. Allerdings nur dann, wenn MitarbeiterInnen diese auch befolgen. Ob Informationssicherheitsvorschriften eingehalten werden oder nicht, hängt von unterschiedlichen Einflussfaktoren ab. In der Literatur werden bereits verschiedene Faktoren und Maßnahmen, die auf die Befolgung von Informationssicherheitsvorschriften einen Einfluss haben, diskutiert. Dazu gehören unter anderem das Informationssicherheitsbewusstsein oder auch die klare Formulierung der Vorschriften. Im Rahmen dieser Studie wurden Faktoren und Maßnahmen aus der Literatur erhoben und qualitative und quantitative Methoden eingesetzt, um deren Relevanz in der Praxis zu evaluieren. In Interviews wurden zusätzliche Faktoren, wie das Verhalten von Stakeholdern, identifiziert. Auch die Vorbildwirkung von ExpertInnen und Persönlichkeitsmerkmale wie die Strukturiertheit der MitarbeiterInnen sind in der Literatur bisher wenig beachtete Faktoren, für die in der Befragungsstudie ein Zusammenhang mit dem Verhalten aufgezeigt werden konnte. Mit Hilfe eines etablierten Verhaltensmodells können diese Zusammenhänge erklärt werden.

**Keywords:** Informationssicherheit, Sicherheitsvorschriften, Bewusstsein, Vorbildwirkung, Persönlichkeitsmerkmale.

## 1 Einleitung

Information zählt zu den wertvollsten Gütern einer Organisation. Dadurch steigt die Bedeutung der Informationssicherheit und Maßnahmen werden etabliert, um Vertraulichkeit, Integrität und Verfügbarkeit (engl. Confidentiality, Integrity, Availability) von Information sicherzustellen und das Unternehmen vor Verlust, Vernichtung, Veröffentlichung, Kopie, Verkauf und sonstigem Missbrauch von Informationen schützen zu können [1], [2]. Organisationen müssen generell ihr Informationssicherheitsrisiko kontrollieren und steuern, um auf unterschiedliche Bedrohungen, wie Angriffe durch Dritte oder fahrlässiges Verhalten von MitarbeiterInnen, reagieren zu können und vertrauliche Daten zu schützen [3–11]. Dies gilt für analoge und digital gespeicherte Daten, allerdings nimmt die Gefahr für

15th International Conference on Wirtschaftsinformatik,
March 08-11, 2020, Potsdam, Germany

https://doi.org/10.30844/wi_2020_l3-krumay

die Informationssicherheit, die von Schwachstellen in Informationssystemen ausgeht, stetig zu.

Aus technischer Sicht wurde das Thema Informationssicherheit bereits intensiv beforscht, dem Individuum als mögliche Schwachstelle wurde bisher allerdings weniger Beachtung geschenkt [12], [13]. Technische Vorkehrungen sind aber nur bedingt wirksam, wenn EndbenutzerInnen – in Unternehmen oder im privaten Umfeld – sich nicht an Vorschriften halten [5–7], [12], [14–17]. Einige Faktoren, die die Einhaltung von Sicherheitsvorschriften fördern wurden bereits intensiv diskutiert, wie zum Beispiel die Etablierung einer entsprechenden Unternehmenskultur, die Förderung des Bewusstseins (engl. Awareness) und die Erreichung von Akzeptanz für Sicherheitsthemen [4], [16]. Allerdings fehlt eine tiefergehende Auseinandersetzung, welche Faktoren und Maßnahmen MitarbeiterInnen zu einem richtlinienkonformen Verhalten motivieren können [4], [7], [16–19].

Ziel dieses Beitrags ist es daher, Faktoren und Maßnahmen zu identifizieren, die das Verhalten - Einhaltung oder Missachtung - der MitarbeiterInnen hinsichtlich Informationssicherheitsvorschriften beeinflussen. Zuerst wird in dieser Studie der aktuelle Stand der Forschung dargestellt und analysiert. Mittels qualitativer Interviews wurden die aus der Literatur erarbeiteten Faktoren und Maßnahmen mit ausgewählten IT-ExpertInnen evaluiert und deren Stellenwert in der Praxis erhoben und ergänzt. Die Ergebnisse wurden in eine nachfolgende Fragebogenuntersuchung aufgenommen, in der MitarbeiterInnen befragt wurden, um die vorliegenden Erkenntnisse zu validieren.

## 2 Stand der Forschung

Für die Informationssicherheit in Organisationen müssen neben technischen Herausforderungen auch die MitarbeiterInnen betrachtet werden [18], da Angreifer gezielt die Schwachstelle „Mensch“ ausnutzen [3], [11], [16]. Diese Angriffe sind dann erfolgreich, wenn Informationssicherheitsvorschriften bewusst oder unbewusst missachtet werden [20]. Um ein gewünschtes Informationssicherheitsniveau zu erreichen, werden Informationssicherheitsvorschriften (Information Security Policies) als sozio-organisatorische Maßnahmen eingesetzt. Informationssicherheitsvorschriften sind ein „statement of the roles and responsibilities of the employees to safeguard the information and technology resources of their organizations” [21]. In einem formellen Dokument wird festgelegt, was erwünschtes und nicht-erwünschtes Verhalten in Bezug auf Informationssicherheit bedeutet [22]. Dieses Dokument muss für alle MitarbeiterInnen zugänglich und verpflichtend zu lesen sein. Mit ihrer Unterschrift erklären diese, das Regelwerk gelesen, verstanden und akzeptiert zu haben. Dadurch soll eine Durchdringung im Unternehmen erreicht werden, die zur Informationssicherheit beiträgt [22]. Diese Vorschriften sind allerdings nicht statisch, sondern müssen regelmäßig den aktuellen Anforderungen angepasst werden, damit das Sicherheitsrisiko minimiert werden kann und mögliche finanzielle Schäden verhindert werden [4]. Allerdings missachten und ignorieren MitarbeiterInnen die

https://doi.org/10.30844/wi_2020_l3-krumay

betrieblichen Informationssicherheitsvorschriften regelmäßig [11], [15]. Faktoren und Maßnahmen die dies begünstigen sind vielfältig und können nur selten voneinander getrennt betrachtet werden. Dazu gehören inhaltliche (z.B. Formulierung), technische (z.B. Zugang zu einer Technologie) und organisatorische Faktoren und Maßnahmen (z.B. Trainings, Motivation), aber auch die Persönlichkeit der MitarbeiterInnen spielt eine bedeutende Rolle.

### 2.1 Inhaltliche, technische und organisatorische Faktoren und Maßnahmen

Ein Faktor, der die Einhaltung von Informationssicherheitsvorschriften beeinflusst, ist deren sorgfältige inhaltliche und sprachliche Gestaltung [20]. Unklare und mehrdeutige Formulierungen führen dazu, dass MitarbeiterInnen die Vorschriften nicht verstehen und daher nicht vollständig oder falsch umsetzen oder sogar ignorieren [20]. Darüber hinaus werden Maßnahmen, mit denen die MitarbeiterInnen vertraut sind, eher befolgt [23]. Auch die Anzahl an Sicherheitsvorschriften und die Frequenz von Änderungen beeinflusst das Verhalten der MitarbeiterInnen [7], [24]. Hier zeigt sich bereits ein erstes Spannungsfeld, da häufige Anpassungen dazu führen, dass MitarbeiterInnen den Änderungen nicht folgen können oder wollen [23], [25], kontinuierliche und zeitlich akkordierte Aktualisierung aber notwendig ist, damit eine entsprechende Umsetzung erfolgen kann [25]. Sicherheitsvorschriften werden aber auch aus technischen Gründen umgangen, wenn zum Beispiel eine notwendige Ressource (z.B. Storage Management zum Speichern von Daten) nicht verfügbar ist, finden MitarbeiterInnen andere, nicht den Vorschriften entsprechende Lösungen (z.B. unsichere, nichtkonforme Medien), um ihre Aufgaben erfüllen zu können [7]. In ähnlicher Art und Weise beeinflusst die empfundene Komplexität einer Vorschrift (z.B. häufige erzwungene Passwortänderungen) das Verhalten [20].

Aus organisatorischer Sicht spielt vor allem der Stellenwert der Sicherheitsvorschriften im Unternehmen eine Rolle. Das Management kann durch regelkonformes Verhalten eine Vorbildwirkung [11], [18], [26] erzielen und dadurch das Verhalten der MitarbeiterInnen beeinflussen [18]. Um die erwünschten Verhaltensmuster in Hinblick auf Informationssicherheit zu verstärken, kann eine Informationssicherheitskultur als Teil der Unternehmenskultur etabliert werden [18]. Diese muss von allen gelebt und ständig in enger Abstimmung zwischen Organisation und den MitarbeiterInnen weiterentwickelt werden [9], [18], um auch im operativen Betrieb eine Verhaltensveränderung zu erreichen [9], [18], [23]. Denn im operativen Betrieb finden sich MitarbeiterInnen häufig in einem Spannungsfeld zwischen Produktivität und Informationssicherheit wieder [7]. Geeignete Instrumente zur Bewertung dieser Situation stehen nur selten zur Verfügung [20]. Bewerten die MitarbeiterInnen das Sicherheitsrisiko als gering, wird basierend auf einer generellen Produktivitätsprämisse der Produktivität der Vorzug gegeben [20]. Auch die handelnden Personen spielen eine bedeutende Rolle. Wird den verantwortlichen Personen vertraut, wirkt sich dies positiv auf die Einhaltung der Informationssicherheitsvorschriften aus und umgekehrt [7], [19], [21], [27], [28]. Häufig werden Sicherheitsvorschriften als zwingend oder bindend definiert [29].

https://doi.org/10.30844/wi_2020_l3-krumay

Insbesondere externe Regularien wie Gesetze verstärken den bindenden Charakter und führen daher oft zu einer strikten Umsetzung [18].

Das reine Vorhandensein einer Liste an Sicherheitsvorschriften reicht nicht aus, um deren Einhaltung zu gewährleisten. In der Literatur aber auch in der Praxis wird daher intensiv das Thema Bewusstsein (engl. Awareness) in Bezug auf Informationssicherheit diskutiert. Ein angemessenes Bewusstsein – ohne die Angemessenheit hier weiter auszuführen – führt zu verbesserter Akzeptanz und dadurch zur Einhaltung von Vorschriften [4], [16]; fehlt dieses Bewusstsein wird das Verhalten negativ beeinflusst [26]. Kommunikation und Schulungen werden als die wichtigsten Maßnahmen zur Bildung von Bewusstsein gesehen [26]. Erfolgt die Kommunikation zur Bewusstseinsbildung über definierte Kanäle und Prozesse (formal-strukturierte Kommunikation), müssen bestimmte Anforderungen an die Inhalte (z.B. Verständlichkeit, Klarheit) erfüllt sein [5]. Auf diese Weise sollen möglichst viele MitarbeiterInnen („One-to-many“) gleichzeitig erreicht werden. Allerdings fühlen sich diese häufig durch diese Massenkommunikation nicht angesprochen [20]. Eine persönliche und individualisierte Kommunikation hat sich als wirkungsvoller erwiesen [20]. Ist die Kommunikation persönlich und informell-unstrukturiert, entsteht bei den MitarbeiterInnen das Gefühl, „auf Augenhöhe“ zu kommunizieren, dadurch wird die Aufmerksamkeit erhöht und das Bewusstsein gesteigert [5]. Allerdings ist informell-unstrukturierte Kommunikation schwer kontrollierbar. Dadurch können sich auf Sicherheitsmythen, die auf Halbwissen basieren, im gesamten Unternehmen verbreiten und erwünschte Verhaltensweisen verdrängen [5], [7]. Schulungen, als weitere Maßnahme zu Bewusstseinsbildung, sollten nicht rein technisch sein, sondern können über Rollenspiele und eine intensive Auseinandersetzung mit realen Vorfällen nachweislich die Bewusstseinsbildung fördern [20].

Neben der Bewusstseinsbildung spielt auch die extrinsische und intrinsische Motivation von MitarbeiterInnen eine große Rolle (z.B. [11], [29–31]). Extrinsische Motivation wird über Anreize (Belohnung – z.B. Belobigungen, Prämien für das Aufdecken von Sicherheitslücken), Sanktionen (Bestrafung – z.B. Dokumentation der Verstöße gegen Sicherheitsvorschriften sowie deren potentielle Auswirkungen, öffentliche Bloßstellung) und Überwachung gesteuert [8], [11], [22], [23]. Ziel ist es jedoch, intrinsische Motivation bei den MitarbeiterInnen hervorzurufen, da diese wirkungsvoller und langfristiger ist. Intrinsische Motivation erzeugt eine emotionale Verpflichtung, regelkonform zu agieren [23]. Sie entsteht, wenn sich MitarbeiterInnen mit dem Unternehmen über gemeinsame Werte identifizieren können [32], wodurch ein Gefühl der Verbundenheit und Einsatzbereitschaft entsteht. Mit Hilfe von Miteinbeziehung in Entscheidungen aber auch durch einen respektvollen Umgang mit den MitarbeiterInnen [29] kann intrinsische Motivation gefördert werden. Im direkten Gegensatz dazu steht die Macht der Organisation; wird diese Organisationsmacht deutlich ausgespielt (z.B. durch Beschränkung der Mitsprache), kann sich das negativ auf die Motivation und die Beziehung zum Unternehmen auswirken [25]. Die Beziehung zwischen Unternehmen und MitarbeiterInnen wird auch als psychologischer Vertrag bezeichnet [33]. Zwischen Unternehmen und MitarbeiterInnen werden bilateral Erwartungen und Verpflichtungen festgelegt, die

https://doi.org/10.30844/wi_2020_l3-krumay

über einen Arbeitsvertrag (der die extrinsischen Faktoren abdeckt) hinausgehen [33]. Die relationalen Inhalte eines psychologischen Vertrags sind eng mit intrinsischen Faktoren (z.B. Verbundenheit mit dem Unternehmen) verknüpft [33]. Die Einhaltung des Vertrags stärkt das Verhältnis zum Unternehmen und indirekt den Willen zum Unternehmenserfolg – zum Beispiel durch Einhaltung der Sicherheitsvorschriften - beizutragen [33].

### 2.2 Inhaltliche, technische und organisatorische Faktoren und Maßnahmen

Zusätzlich zu Anreizen und Maßnahmen beeinflussen auch individuelle Faktoren direkt die Annahme und Umsetzung von Sicherheitsvorschriften. Generell unterscheidet man in diesem Kontext zwischen schneller bzw. früher Annahme („early conformers"), langsamer bzw. später Annahme („late conformers") oder Verweigerung („nonconformers") [4]. Neben den kognitiven Fähigkeiten (z.B. Auffassungsgabe) [22] beeinflussen auch Sozialisierung, persönliche Wertvorstellung sowie die persönliche Wahrnehmung [16], wie Vorschriften angenommen werden. Ein direkter Zusammenhang zwischen individuellen Fähigkeiten und anderen Faktoren besteht zum Beispiel in Hinblick auf Lesbarkeit und Verständlichkeit der Vorschriften, aber auch der Fähigkeit, Sinn und Zweck erkennen zu können [7], [11], [20]. Kann die Bedeutung des Dokuments [11], [15] und die Konsequenzen der Missachtung von Vorschriften von den MitarbeiterInnen entsprechend beurteilt werden [10], hat dies ebenfalls Einfluss auf das Verhalten. Dieses Verständnis kann durch Darstellung von Sinn und Wichtigkeit der Sicherheitsvorschriften (z.B. durch Aufzeigen der finanziellen Auswirkungen [18]) gefördert werden. Verständnis, Vertrautheit und die Fähigkeit mit einem Sicherheitsvorfall richtig umzugehen beeinflussen ebenfalls das Verhalten [10], [11]. Stoßen MitarbeiterInnen an ihre persönlichen Grenzen (z.B. durch häufiges Wechseln von Passwörtern), führt das zu Missachtung der Sicherheitsvorschriften sowie Stress und weiter zu sinkender Produktivität, Arbeitsmoral und Jobzufriedenheit [7], [24]. Gerade Arbeitszufriedenheit und Wohlbefinden haben aber Einfluss auf die Einhaltung von Vorschriften [24].

Neben den bereits beschriebenen Faktoren spielt auf individueller Ebene die Selbstwirksamkeitserwartung (engl. perceived self-efficacy) eine bedeutende Rolle [34]. Darunter versteht man die Erwartung eines Individuums, eigene Kompetenzen zur erfolgreichen Ausführung einer Handlung einsetzen zu können [34], [35]. Erwartet jemand von sich selbst in einer gewissen Situation selbständig handeln zu können, führt das dazu, dass diese Person auch davon überzeugt ist, die Situation (und die Welt) beeinflussen und verändern zu können [34], [35]. Werden MitarbeiterInnen in ihrer Selbstwirksamkeit hinsichtlich Informationssicherheit bestärkt, so werden sie aktiv zur Sicherheit beitragen [29]. Das Konzept der Selbstwirksamkeitserwartung findet sich in vielen verhaltenstheoretischen Erklärungsmodellen und Theorien wieder (z.B. Social Cognitive Theory [34], [35], Rational Choice Theory [33], [36], Social Bonding Theory [11], [30], Involvement-Commitment-Theory [37], [38], Theory of Planned Behavior [16], [39], [40], Protection Motivation Theory, [29], [31], General Deterrence Theory [41], Norm Activation Theory [42], Theory of Social Norms [43]).

https://doi.org/10.30844/wi_2020_l3-krumay

Diese Ansätze können zur Klärung und Darstellung des Verhaltens der MitarbeiterInnen im Kontext der Informationssicherheit herangezogen werden [21].

## 3 Methodischer Ansatz

Im Rahmen dieser Studie wurde basierend auf einer Literaturrecherche ein Interviewleitfaden entwickelt. Mit Hilfe von qualitativen Interviews wurden die in der Literatur ermittelten Faktoren und Maßnahmen evaluiert und erweitert. Zusätzlich wurde eine quantitative Befragungsstudie durchgeführt, um die Ergebnisse zu validieren.

Der Interviewleitfaden enthielt neben einer Einstiegsfrage und Fragen zur Person (Verantwortlichkeit, Abteilung, Anzahl MitarbeiterInnen in der Abteilung) und zum Unternehmen (Branche, Anzahl MitarbeiterInnen) vor allem Fragen zur eigenen Einschätzung (1 – 5) der InterviewpartnerInnen hinsichtlich der Bedeutung von Informationssicherheit für das Unternehmen und den eigenen Aufgabenbereich. Danach wurden offene Fragen zu den Informationssicherheitsvorschriften, deren Miss- oder Beachtung, Einschätzung des durch Missachtung entstehenden Risikos sowie zur Beurteilung des eigenen Verhaltens im Interviewleitfaden hinterlegt. Insgesamt wurden sechs Interviews (I1 – I6) mit sieben ExpertInnen mit einer durchschnittlichen Interviewdauer von 70 min. (min. 20 Minuten, max. 2,5 Stunden) geführt. Die Interviews erfolgten in einer Zeitspanne von drei Monaten und fanden in den Unternehmen der InterviewpartnerInnen statt. Von den Unternehmen sind je zwei im Bereich IT Security Consulting bzw. IT Consulting tätig, ein Unternehmen gehört der IT-Dienstleistungsbranche an und das sechste Unternehmen ist ein Finanzinstitut. Vier der InterviewpartnerInnen sind Teil der Geschäftsführung, zwei sind leitende Angestellte sowie ein/e FilialleiterIn (siehe Tabelle 1).

**Tabelle 1.** Beschreibung der InterviewpartnerInnen

| *No.* | *Position* | *Branche* | *Größe* | *Datum* |
|---|---|---|---|---|
| I1 | Geschäftsführung | IT Dienstleistungen | KMU | 15.12.2017 |
| I2 | FilialleiterIn | Finanzinstitut | Zweigstelle | 10.01.2018 |
| I3a / I3b | Leitende Angestellte | IT Security Consulting | Konzern | 11.01.2018 |
| I4 | Geschäftsführung | IT Consulting | KMU | 12.01.2018 |
| I5 | Geschäftsführung | IT Security Consulting | KMU | 25.01.2018 |
| I6 | Geschäftsführung | IT Consulting | KMU | 05.02.2018 |

Die Interviews wurden elektronisch aufgezeichnet, transkribiert und mittels qualitativer Inhaltsanalyse nach Mayring [44] analysiert. Dabei wurden sowohl deduktive Kategorienbildung basierend auf der Literatur, als auch induktive Kategorienbildung eingesetzt. Die Reliabilität von qualitativen Ansätzen wird häufig mittels eines Übereinstimmungs- bzw. Reliabilitätskoeffizienten ermittelt [45]. In diesem Fall liegt die Interrater-Reliabilität zwischen den beteiligten ForscherInnen bei 0,73 und die Intrarater-Reliabilität bei 0,97 [45].

https://doi.org/10.30844/wi_2020_l3-krumay

Um die Ergebnisse abzusichern und quantitativ zu validieren wurde eine Befragungsstudie durchgeführt. Der Fragebogen wurde basierend auf den Ergebnissen der qualitativen Interviews entworfen, einem Pre-Test unterzogen, überarbeitet und in einem Online-Tool (LimeSurvey) umgesetzt. Der Fragebogen enthielt (neben Fragen zum Unternehmen und zur Person) Fragen zur Nutzung von Computern im Unternehmen und privat, zur Arbeitsplatzumgebung, eigenen Umgang mit Sicherheitsvorschriften, Persönlichkeit sowie Sicherheit und Daten am Arbeitsplatz (siehe Anhang A). Die Fragen zur Persönlichkeit sowie zu Sicherheit und Daten am Arbeitsplatz wurden Likert-skaliert (5-teilig: trifft völlig zu / trifft eher zu / trifft teilweise zu / trifft eher nicht zu / trifft nicht zu / weiß ich nicht). Die Einladung zum Fragebogen erging an rund 500 Personen (selektives Sampling), die gebeten wurden, den Link weiter zu geben (Snowball Sampling). Die Einladung erfolgte per Mail und über diverse soziale Netzwerke. Die Umfrage war 21 Tage lang verfügbar und wurde von 201 Personen beantwortet (99 Männer; 102 Frauen zwischen 17 und 65 Jahren). Die TeilnehmerInnen unterscheiden sich hinsichtlich Bildungsstand (höchste abgeschlossene Schulbildung – Pflichtschule: 19 %, mittlere- oder höhere Schule: 44 %; Hochschule: 37 %) und sind in unterschiedlichen Sektoren tätig (am häufigsten vertretene Sektoren: Öffentlicher Dienst: 26 %, IT-Branche: 23 %; Dienstleistungssektor: 18 %). Neben einer Assoziationsanalyse wurden Zusammenhangsanalysen mittels Mann-Withney-U- und Chi-Quadrat-Tests durchgeführt, dafür wurden die Likert-skalierten Items gewichtet. Untersucht wurden Zusammenhänge zwischen persönlichen Merkmalen sowie den einzelnen Faktoren in Bezug auf das Verhalten hinsichtlich Sicherheitsvorschriften.

# 4 Ergebnisse

Die Ergebnisse werden getrennt nach den eingesetzten Methoden dargestellt. Kurz zusammengefasst wurden in den Interviews Verständlichkeit der Vorschriften, Einfluss auf den operativen Betrieb sowie Steigerung des Bewusstseins thematisiert. Zusätzlich zu den in der Literatur vorkommenden Faktoren wurden demographisch-kulturelle Faktoren, die Vorbildwirkung von ExpertInnen und der Einfluss von Stakeholdern (Kunden) diskutiert. Die Auswertung der Fragebögen zeigt, dass die Befragten ihr Verhalten positiv beurteilen, aber auf konkrete Szenarien bezogen allgemeingültige Sicherheitsvorschriften missachtet werden. Signifikante Zusammenhänge konnten nur vereinzelt festgestellt werden.

## 4.1 Ergebnisse der Interviews

Im Rahmen der Interviews wurden nicht nur Faktoren erhoben bzw. evaluiert, sondern auch deren Bedeutung und Zusammenhänge von den InterviewpartnerInnen ermittelt. Verständlichkeit und Klarheit der Vorschriften wurden dabei als wichtige Faktoren für Be- oder Missachtung von Informationssicherheitsvorschriften in vier Interviews genannt (I3a & b, I4, I5, I6). In Bezug auf die Formulierung wurde auch darauf hingewiesen, dass die Vorschriften die gewöhnliche Geschäftstätigkeit nicht

https://doi.org/10.30844/wi_2020_l3-krumay

behindern dürfen und sie deshalb manchmal, „schwammig formuliert werden müssen“ (I3a). Trotzdem wurden strikte Vorgaben als einfacher zu befolgen eingeschätzt (I2, I5). In zwei Interviews wurde angeführt, dass den MitarbeiterInnen mögliche Konsequenzen nicht bewusst sind und dies zu einem Fehlverhalten führt (I1, I4). Auch das Fehlen von Alternativen (z.B. ein Verbot von externen Cloudservices ohne ein entsprechendes internes Angebot) wurde als Faktor genannt (I3a, I4). Externe Einflüsse, z.B. wenn der Datenaustausch von Dritten über ein bestimmtes Cloudservice forciert wird, verunsichern MitarbeiterInnen hinsichtlich der eigenen Vorschriften und deren Einhaltung, da die Geschäftsbeziehung in Konkurrenz zur Sicherheit steht (I3a & b, I5). In drei Interviews wurde erwähnt, dass Mitarbeiterinnen die ständig neu auftretenden Risiken nicht richtig einschätzen können und deshalb Vorschriften missachten (I1, I2, I4). Thematisiert wurde darüber hinaus, dass Routinetätigkeiten (I5), das Verhalten von Kunden (z.B. Forderung nach schneller Abwicklung) (I1) sowie die fehlende Unterstützung durch das Management (I2) zu einer Missachtung führen können. Auch die Nutzung von privaten Geräten im Unternehmen („bring your own device“) bzw. umgekehrt die Nutzung von Geräten des Unternehmens für private Zwecke wurden genannt (I4).

**Tabelle 2.** Abdeckung der Faktoren aus der Literatur (Lit.) in den Interviews (Int., o = kaum Abdeckung, + = geringe Abdeckung, ++ = mittlere Abdeckung, +++ hohe Abdeckung)

| *Thema* | *Int.* | *Thema* | *Int.* |
|---|---|---|---|
| Aktualität [11], [15], [25] | ++ | Risikoeinschätzung [20] | ++ |
| Akzeptanz [4], [16], [26] | ++ | Rollenspiele [20] | + |
| Arbeitsmoral [24] | ++ | Schulungen [26] | +++ |
| Auffassungsgabe [22] | + | Selbstwirksamkeit [29], [34] | + |
| Bedeutung erkennen [11], [15] | + | Sozialisierung [16] | o |
| Beteiligung [29] | + | *Stakeholder* | + |
| Bewusstsein [4], [16], [26] | +++ | Technische Gegebenheiten [7], [25] | ++ |
| Beziehung zum Unternehmen [33] | ++ | Überforderung [7] | + |
| Bloßstellung [23] | o | Überzeugung [29] | ++ |
| Eigenverantwortliches Handeln [29] | ++ | Umgang mit Verstößen [10], [11] | ++ |
| Einbeziehung [29] | + | Unternehmenskultur [9], [18], [23] | +++ |
| Einsatzbereitschaft [29] | + | Unterstützung des Managements [11], [18], [26] | +++ |
| Geschwindigkeit [4] | o | Verbundenheit [29] | o |
| Halbwissen [5] | + | Verpflichtend zu lesen [22] | + |
| Jobzufriedenheit [24] | ++ | Verständlichkeit [20] | +++ |
| Kommunikation [5] | ++ | Verständnis [7], [10], [11], [20] | +++ |
| Konsequenzen [10] | ++ | *Vorbildwirkung von ExpertInnen* | +++ |
| Motivation [11], [23], [29–31] | ++ | Wahrnehmung [16] | + |
| Neuheit der Maßnahmen [23] | + | Wertvorstellung [16] | o |
| Organisationsmacht [25] | o | Wirtschaftliche Bedeutung [18] | ++ |
| Person/Persönlichkeit [7], [19], [21], [27], [28] | + | Wohlbefinden am Arbeitsplatz [24] | + |
| | | Zahl der Vorschriften [24] | + |

https://doi.org/10.30844/wi_2020_l3-krumay

| *Thema* | *Int.* | *Thema* | *Int.* |
|---|---|---|---|
| Produktivität [7], [20] | ++ | Zugänglichkeit [22] | + |
| Reale Fälle [20] | ++ | Zwang [18], [29] | + |

Als wirksamste Maßnahme um eine Beachtung der Sicherheitsvorschriften zu erreichen gilt die Steigerung des Sicherheitsbewusstseins (I1, I2, I4, I6). In drei Interviews (I3a & b, I4, I5) wurden Kommunikation und Schulungen sowie das Schaffen von technischen Voraussetzungen genannt. Zwei InterviewpartnerInnen (I3a, I5) waren der Meinung, dass Fehlverhalten nicht toleriert und zudem Sanktionen gesetzt werden sollten. Die Schaffung von klaren Richtlinien und getrennt davon Handlungsempfehlungen (als Vereinfachung) wurde von zwei InterviewpartnerInnen (I1, I6) als adäquate Maßnahme genannt. Die Darstellung von echten Beispielfällen bzw. aktuellen Anlassfällen (I3b), der Einsatz von Kurzvideos (I4), die Schaffung einer entsprechenden Kultur (I3a) bzw. Einbettung von Informationssicherheit in die Vision des Unternehmens (I3b) wurde ebenfalls empfohlen. Besonders erwähnt wurde die Vorbildwirkung von ExpertInnen (I2, I3a & b, I5, I6). Zwei InterviewpartnerInnen (I1, I2) äußerten, dass die Persönlichkeit der MitarbeiterInnen und deren Bildung starken Einfluss auf das regelkonforme Verhalten haben. Sie äußerten die Vermutung, dass gebildete MitarbeiterInnen die Vorschriften missachten, weil sie glauben es besser zu wissen (I1). In einem Interview (I2) wurde explizit zwischen weniger gebildeten MitarbeiterInnen („wissen es nicht besser“), „Halbgebildeten“ („machen ihre eigenen Regeln“), ExpertInnen („fühlen sich eingeschränkt und umgehen die Maßnahmen, weil sie wissen wie es geht“) und dem Top-Management („dafür gibt es immer Sonderkonditionen”) unterschieden. Es wurde hervorgehoben, dass insbesondere die Vorbildwirkung von ExpertInnen und Top-Management entscheidend ist. Auch kulturelle Unterschiede beeinflussen nach Ansicht der InterviewpartnerInnen das Verhalten (I4). Der Einschätzung nach beachten ältere MitarbeiterInnen eher Vorschriften (I3b), aber auch das Geschlecht (I4) wurde als Einflussfaktor genannt. In einem Interview (I2) wurde festgestellt, dass MitarbeiterInnen mittlerweile Sicherheitsberechtigungen nicht mehr annehmen, um bestimmte Aufgaben nicht übernehmen zu müssen. Tabelle 2 fasst das Vorkommen der Faktoren in der Literatur und deren Repräsentation in den Interviews (Int.) in strukturierter Weise zusammen, wobei eine Einstufung von kaum (wurde in den Interviews nicht oder nur am Rande erwähnt) bis hohe Abdeckung (wurde ausführlich in mehreren Interviews diskutiert) vorgenommen wurde. Faktoren, die nicht eindeutig in der Literatur vorkommen, aber aus den Interviews exzerpiert wurden, sind kursiv dargestellt.

### 4.2 Ergebnisse der Interviews

Die hier dargestellten Ergebnisse fokussieren auf Verhalten, demographische Unterschiede, Persönlichkeitsmerkmale sowie ausgewählte Faktoren aus der Literatur, da andere, ebenfalls erhobene Faktoren (Computernutzung, Arbeitsumfeld) sowohl demographisch als auch hinsichtlich Zusammenhängen keine relevanten Ergebnisse aufzeigen. Wie bereits erwähnt beurteilten die Befragten ihr eigenes Verhalten als

https://doi.org/10.30844/wi_2020_l3-krumay

durchaus positiv. So gaben 37 % der TeilnehmerInnen an, sich „völlig“ und 50 % sich „eher“ an die Sicherheitsvorschriften zu halten („Ich halte mich an Sicherheitsvorschriften“), während niemand angab, sich nicht („trifft nicht zu“) an Sicherheitsvorschriften zu halten. Allerdings zeigen die Ergebnisse, dass allgemeine, im Fragebogen operationalisierte Szenarien häufig nicht befolgt werden (Angabe „trifft völlig zu“ - Verwendung eines Verschlüsselungsverfahrens zur Kennwortabsicherung: 10 %; Weitergabe des Passworts „für Notfälle“ an Personen aus dem familiären Umkreis: 25 %; Verwendung eines Passwortmanagers: 25 %). Manche Sicherheitsvorschriften werden von einem Großteil der TeilnehmerInnen umgesetzt (Passwörter werden nicht notiert: 53 %; Passwörter werden nicht an vertrauenswürdige Personen im Unternehmen weitergegeben: 53 %; Verwendung unterschiedlicher Passwörter je Internetdienst: 65 %). Das Wissen hinsichtlich allgemeiner Informationssicherheitsrisiken ist unter den Befragten nicht sehr ausgeprägt (Angabe „trifft völlig zu“: Daten sind auf einer formatierten Festplatte nicht permanent gelöscht: 25 %; E-Mails, die nicht im Spam-Ordner landen, sind nicht automatisch als sicher einzustufen: 25 %). Sicherheitsvorschriften im eigenen Unternehmen wurden von zwei Drittel der TeilnehmerInnen als angemessen streng aber nur von 40 % als praxisorientiert eingeschätzt. Ebenfalls 40 % gaben an zu wissen, wo die Sicherheitsvorschriften zu finden sind. Die Frage nach den Konsequenzen („Die Konsequenzen bei Nicht-Befolgung der Sicherheitsvorschriften sind klar geregelt“) wurde unterschiedlich beantwortet („trifft völlig zu“: 10 %; „trifft eher zu“: 18 %; „trifft teilweise zu“: 22 %; „trifft eher nicht zu“: 18 %; „trifft nicht zu“: 10 %). Besonders fällt auf, dass häufig keine Angaben gemacht wurde („weiß nicht“: 22 %).

In Hinblick auf das Alter der TeilnehmerInnen werden nur die häufigsten Antworten je Altersgruppe dokumentiert. Auffällig war, dass jüngere TeilnehmerInnen angaben, sich nur teilweise an Sicherheitsvorschriften zu halten (60 % in der Altersgruppe bis 20 Jahre), während mit zunehmendem Alter die Häufigkeiten sich in Richtung „trifft eher zu“ bzw. „triff völlig zu“ verlagert (21 – 30 Jahre: 63,6 % „trifft eher zu“, 31 - 40 Jahre: 41,2 % „trifft eher zu“; 41 - 50 Jahre: 52,1 % trifft völlig zu; über 51 Jahre: 45,9 % „trifft völlig zu“, 51,4 % „trifft eher zu“). Rein deskriptiv könnte man also sagen, dass jüngere TeilnehmerInnen Sicherheitsvorschriften eher missachten. Bei den Frauen geben fast 50 % an, sich völlig an Sicherheitsvorschriften zu halten, bei den Männern nur rund 25 %. Kumuliert man die Antwortmöglichkeiten „trifft völlig zu“ und „trifft eher zu“ gleicht sich dieser Unterschied aber aus. Hinsichtlich Sektoren gaben 49 % der TeilnehmerInnen im öffentlichen Dienst an, sich völlig an Sicherheitsvorschriften zu halten (IT: 25 %; Dienstleistungen: 18 %). Während TeilnehmerInnen ohne Hochschulabschluss überwiegend angaben, sich vollständig an Sicherheitsvorschriften zu halten (Pflichtschule: 47,4%; Mittlere bzw. höhere Schule: 42,7 %), gaben nur 25,7 % der HochschulabsolventInnen an, sich immer an Sicherheitsvorschriften zu halten, 66,2 % gaben an, sich nur „eher“ daran zu halten. Hinsichtlich der persönlichen Faktoren gaben unter den TeilnehmerInnen 41,8 % an, strukturiert und ordentlich zu sein („trifft völlig zu“) und sich an Vorgaben zu halten, auch wenn sie die Erfüllung der Aufgaben erschweren (41,8 %). Andere individuelle

https://doi.org/10.30844/wi_2020_l3-krumay

Faktoren wie Kritikfähigkeit, Fehlerkultur und Risikofreude ergaben kein eindeutiges Bild. Allerdings gaben die TeilnehmerInnen an, dass die Unternehmenskultur (35,6 %) und Wohlbefinden im Unternehmen (38,8 %) Einfluss auf ihr Verhalten haben. Hinsichtlich ExpertInnen gaben 80 % der TeilnehmerInnen an, dass sich ihrer Wahrnehmung nach diese an Sicherheitsvorschriften halten. Rund ein Drittel der Unternehmen organisiert laut Angaben der TeilnehmerInnen keine Sicherheitstrainings, allerdings fördert mehr als die Hälfte der Unternehmen das Sicherheitsbewusstsein.

Die Ergebnisse der Befragungsstudie wurden auch auf Zusammenhänge zwischen unterschiedlichen Faktoren und dem Verhalten („Ich halte mich an Sicherheitsvorschriften“) getestet. Auch wenn die deskriptive Auswertung Zusammenhänge vermuten lässt, sind nur wenige tatsächlich feststellbar. So konnte zum Beispiel kein eindeutiger Zusammenhang zwischen der eigenen Einschätzung hinsichtlich Einhaltung von Sicherheitsvorschriften („Ich halte mich an Sicherheitsvorschriften“) und der tatsächlichen Einhaltung (operationalisiert in Form von allgemeinen Sicherheitsvorschriften) im vorliegenden Sample festgestellt werden. Hinsichtlich demographischer Merkmale konnte ein schwacher Zusammenhang zwischen Verhalten und Bildungsstand festgestellt werden, der vermuten lässt, dass mit der Höhe der Bildung die Einhaltung von Sicherheitsvorschriften abnimmt. Stellt man Persönlichkeitsmerkmale der Befolgung von Vorschriften gegenüber, findet sich ein positiver Zusammenhang zwischen Strukturiertheit und der Befolgung von Vorschriften. Darüber hinaus korrelieren das beobachtete Verhalten von ExpertInnen mit dem eigenen Verhalten (Einhaltung von Sicherheitsvorschriften) positiv.

## 5 Diskussion und Fazit

Neben vielfältigen technischen Maßnahmen zur Steigerung der Informationssicherheit darf der menschliche Aspekt nicht vernachlässigt werden. Ziel des Beitrags war es, mögliche persönlichkeitsbezogene Faktoren und Maßnahmen, die die Einhaltung oder Missachtung von Sicherheitsvorschriften beeinflussen, zu identifizieren. Diese Studie trägt somit dazu bei, das Wissen über individuelle Einflussfaktoren und Maßnahmen in Bezug auf Einhaltung von Informationssicherheitsmaßnahmen zu erweitern. Aus der Literatur wurden verschiedene Faktoren und Maßnahmen abgeleitet, die den Informationssicherheitsvorschriften selbst (Formulierung) aber auch der Organisation (Verantwortung und Vorbildwirkung; Struktur und Maßnahmen) zugeordnet werden können, und die mit Persönlichkeit und Wahrnehmungen der MitarbeiterInnen interagieren. Organisationen setzen Maßnahmen, wie Schulungen zur Steigerung des Informationssicherheitsbewusstseins, um das Verhalten der MitarbeiterInnen in die gewünschte Richtung zu lenken. Fehlende Unterstützung durch das Management, das Fehlen einer entsprechenden Unternehmenskultur und unzureichende Vermittlung der Relevanz der Vorschriften führen dazu, dass sich MitarbeiterInnen nicht zur Einhaltung von Sicherheitsvorschriften verpflichtet fühlen. Individuelle Faktoren der MitarbeiterInnen müssen dabei verstärkt beachtet werden. In den Interviews wurden die meisten in der Literatur identifizierten Faktoren und Maßnahmen validiert. Dabei

https://doi.org/10.30844/wi_2020_l3-krumay

wurden behördliche Vorschriften („Zwang“), unternehmensinterne Sanktionen, die durch Abschreckung regelkonformes Verhalten herbeiführen sollen sowie übertrieben strenge Vorschriften von den InterviewpartnerInnen kritisch betrachtet. Aus den Interviews kann auch eine Art Wissens- und Vertrauenshierarchie abgeleitet werden, die sich vereinfacht auf „Nichtwissende“, „Halbwissende“, „ExpertInnen“ und „Top-Management“ zusammenfassen lässt. Diese Strukturierung und die Unterscheidung in „selbsternannte“ und wahrgenommene ExpertInnen und deren Einfluss wird in der Literatur bisher nicht ausführlich diskutiert. Daher wurde diese Fragestellung, wie die Vorbildwirkung von ExpertInnen das Verhalten beeinflusst, in die Befragungsstudie aufgenommen. Darüber hinaus wurde ein möglicher Zusammenhang mit weiteren demographischen und persönlichen Faktoren im Rahmen der Befragungsstudie untersucht, die in den Interviews genannt wurden. Ein in der Literatur positiv angenommener Zusammenhang zwischen der Abhaltung von Sicherheitstrainings und des Informationssicherheitsbewusstseins konnte interessanterweise nicht bestätigt werden. Dies kann daran liegen, dass die Befragten die Abhaltung von Sicherheitstrainings nicht als Förderung des Informationssicherheitsbewusstseins erkennen. Auch demographische Zusammenhänge sind nicht erkennbar, einzig der Bildungsstand scheint einen geringen Einfluss auf das Verhalten zu haben. Je höher der Bildungsstand, umso eher werden Sicherheitsvorschriften nur teilweise befolgt. Dies kann mit der Lebenssituation und der generellen Neigung, Dinge zu hinterfragen, zusammenhängen, oder auch mit einem unstimmigen Selbstbild in Bezug auf eigene Kompetenzen. In der Literatur wurde allerdings bisher ein signifikanter Einfluss des Ausbildungsniveaus nicht bestätigt [46]. Hinsichtlich der Persönlichkeitsmerkmale wurde eine positive Korrelation zwischen der eigenen (empfundenen) Strukturiertheit der TeilnehmerInnen und der Einhaltung von Sicherheitsvorschriften festgestellt. Dies kann einerseits aus dem Blickwinkel des psychologischen Vertrags betrachtet werden. Die Erwartungshaltungen beider Akteure halten sich insofern die Waage, da das Unternehmen strukturiertes Arbeiten erwartet und daher Vorschriften zur Verfügung stellt. Dies geht einher mit der Erwartungshaltung des Individuums, eine strukturierte Arbeitsumgebung vom Unternehmen zur Verfügung gestellt zu bekommen. Andererseits kann Strukturiertheit mit stärkerer Arbeitsorganisation und der Befolgung entsprechender Prozesse assoziiert werden. Die Vorbildwirkung von ExpertInnen, für die ein Zusammenhang mit der Einhaltung von Vorschriften festgestellt wurde, wurde bisher in der Literatur nicht ausführlich betrachtet. Analog zur Vorbildwirkung des Top-Managements [11], [18], [26], [46], kann auch das regelkonforme Verhalten von ExpertInnen MitarbeiterInnen dazu motivieren, sich selbst regelkonform zu verhalten. In einigen psychologischen Erklärungsmodellen wird das Lernen von Verhaltensmustern thematisiert, z.B. in der Social Cognitive Theory [35]. Vereinfacht gesagt wird eigenes Verhalten durch Beobachtung menschlichen Verhaltens gelernt, sozusagen basierend auf einem Modell (z.B. [34], [35]). Dabei produzieren und konsumieren alle Beteiligten, abhängig von sozio-strukturalen Einflüssen [35]. Von diesen Einflüssen spielt hier vor allem die Beziehung zu den ExpertInnen eine wichtige Rolle. Erkenntnisse, die sich direkt auf die Selbstwirksamkeitserwartung [34] beziehen, konnten im Rahmen dieser Studie nicht gewonnen werden. Diese

https://doi.org/10.30844/wi_2020_l3-krumay

könnten in einer Studie unter Einbeziehung der Social Cognitive Theory weiter vertieft werden.

## Literatur


1. Kersten, H., Reuter, J., Schröder, K.-W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: der Weg zur Zertifizierung. Springer Vieweg, Wiesbaden (2013).
2. ISO/IEC 27001:2013 Requirements. International Organization for Standardization (2013).
3. Aurigemma, S., Panko, R.: A composite framework for behavioral compliance with information security policies. In: 2012 45th Hawaii International Conference on System Sciences. pp. 3248–3257. IEEE (2012).
4. Bélanger, F., Collignon, S., Enget, K., Negangard, E.: Determinants of early conformance with information security policies. Information & Management. 54, 887–901 (2017).
5. Dang-Pham, D., Pittayachawan, S., Bruno, V.: Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. Computers in Human Behavior. 67, 196–206 (2017).
6. Kaur, J., Mustafa, N.: Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In: 2013 International Conference on Research and Innovation in Information Systems (ICRIIS). pp. 286–290. IEEE (2013).
7. Kirlappos, I., Beautement, A., Sasse, M.A.: "Comply or Die" Is Dead: Long Live Security-Aware Principal Agents. In: Adams, A.A., Brenner, M., and Smith, M. (eds.) Financial Cryptography and Data Security. pp. 70–82. Springer Berlin Heidelberg (2013).
8. Kolkowska, E., Karlsson, F., Hedström, K.: Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. The Journal of Strategic Information Systems. 26, 39–57 (2017).
9. Mahfuth, A., Yussof, S., Baker, A.A., Ali, N.: A systematic literature review: Information security culture. In: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). pp. 1–6. IEEE (2017).
10. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security. 66, 40–51 (2017).
11. Safa, N.S., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Computers & Security. 56, 70–82 (2016).
12. Maqousi, A., Balikhina, T., Mackay, M.: An effective method for information security awareness raising initiatives. International Journal of Computer Science & Information Technology. 5, 63 (2013).
13. Öğütçü, G., Testik, Ö.M., Chouseinoglou, O.: Analysis of personal information security behavior and awareness. Computers & Security. 56, 83–93 (2016).
14. Li, L., He, W., Xu, L., Ivan, A., Anwar, M., Yuan, X.: Does explicit information security policy affect employees' cyber security behavior? A pilot study. In: 2014 Enterprise Systems Conference. pp. 169–173. IEEE (2014).


https://doi.org/10.30844/wi_2020_l3-krumay

15. Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E.: Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems. 24, 38–58 (2015). https://doi.org/10.1057/ejis.2013.27.
16. Ifinedo, P.: Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management. 51, 69–79 (2014). https://doi.org/10.1016/j.im.2013.10.001.
17. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. 34, 523 (2010). https://doi.org/10.2307/25750690.
18. Fagade, T., Tryfonas, T.: Security by compliance? A study of insider threat implications for Nigerian banks. In: International Conference on Human Aspects of Information Security, Privacy, and Trust. pp. 128–139. Springer (2016).
19. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Information Management & Computer Security. 8, 31–41 (2000).
20. Bauer, S., Bernroider, E.W.N., Chudzikowski, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. Computers & Security. 68, 145–159 (2017). https://doi.org/10.1016/j.cose.2017.04.009.
21. Topa, I., Karyda, M.: Identifying factors that influence employees' security behavior for enhancing ISP compliance. In: International Conference on Trust and Privacy in Digital Business. pp. 169–179. Springer (2015).
22. Alotaibi, M., Furnell, S., Clarke, N.: Information security policies: A review of challenges and influencing factors. In: 11th International Conference for Internet Technology and Secured Transactions (2016).
23. Harkins, M.: Managing risk and information security: protect to enable. Springer (2013).
24. Lee, C.H., Geng, X., Raghunathan, S.: Mandatory Standards and Organizational Information Security. Information Systems Research. 27, 70–86 (2016). https://doi.org/10.1287/isre.2015.0607.
25. Kolkowska, E., Dhillon, G.: Organizational power and information security rule compliance. Computers & Security. 33, 3–11 (2013).
26. Chaudhry, P.E., Chaudhry, S.S., Reese, R., Jones, D.S.: Enterprise information systems security: a conceptual framework. In: Re-Conceptualizing Enterprise Information Systems. pp. 118–128. Springer (2012).
27. Furnell, S.M., Gennatou, M., Dowland, P.S.: A prototype tool for information security awareness and training. Logistics Information Management. 15, 352–357 (2002).
28. Lee, J., Lee, Y.: A holistic model of computer abuse within organizations. Information management & computer security. 10, 57–63 (2002).
29. Dang-Pham, D., Pittayachawan, S., Bruno, V.: Exploring behavioral information security networks in an organizational context: An empirical case study. Journal of Information Security and Applications. 34, 46–62 (2017). https://doi.org/10.1016/j.jisa.2016.06.002.
30. Hirschi, T.: Causes of delinquency. Routledge (2017).
31. Rogers, R.W.: A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology. 91, 93–114 (1975). https://doi.org/10.1080/00223980.1975.9915803.

32. Calder, B.J., Staw, B.M.: Self-perception of intrinsic and extrinsic motivation. Journal of Personality and Social Psychology. 31, 599–605 (1975). https://doi.org/10.1037/h0077100.
33. Han, J., Kim, Y.J., Kim, H.: An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. Computers & Security. 66, 52–65 (2017).
34. Bandura, A.: Self-efficacy mechanism in human agency. American Psychologist. 37, 122–147 (1982). https://doi.org/10.1037/0003-066X.37.2.122.
35. Compeau, D.R., Higgins, C.A.: Application of Social Cognitive Theory to Training for Computer Skills. Information Systems Research. 6, 118–143 (1995).
36. Scott, J.: Understanding Contemporary Society. Theories of the Present. In: Rational Choice Theory. pp. 126–132 (2000).
37. Beatty, S.E., Homer, P., Kahle, L.A.: The Involvement-Commitment Model: Theory and Implications. Journal of Business Research. 16, 149–167 (1988).
38. Lee, S.M., Lee, S.-G., Yoo, S.: An integrative model of computer abuse based on social control and general deterrence theories. Information & Management. 41, 707–718 (2004).
39. Ajzen, I.: The theory of planned behavior. Organizational Behavior and Human Decision Processes. 50, 179–211 (1991). https://doi.org/10.1016/0749-5978(91)90020-T.
40. Sommestad, T., Hallberg, J.: A review of the theory of planned behaviour in the context of information security policy compliance. In: IFIP International Information Security Conference. pp. 257–271. Springer (2013).
41. Straub, D.W., Welke, R.J.: Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly. 22, 441 (1998). https://doi.org/10.2307/249551.
42. Yazdanmehr, A., Wang, J.: Employees' information security policy compliance: A norm activation perspective. Decision Support Systems. 92, 36–46 (2016).
43. Elster, J.: Social Norms and Economic Theory. Journal of Economic Perspectives. 3, 99–117 (1989). https://doi.org/10.1257/jep.3.4.99.
44. Mayring, P.: Qualitative Inhaltsanalyse. In: Mey, G. and Mruck, K. (eds.) Handbuch Qualitative Forschung in der Psychologie. pp. 601–613. VS Verlag für Sozialwissenschaften, Wiesbaden (2010). https://doi.org/10.1007/978-3-531-92052-8_42.
45. Neuendorf, K.A.: The Content Analysis Guidebook. Sage (2016).
46. Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*: Managing Employee Compliance with Information Security Policies. Decision Sciences. 43, 615–660 (2012). https://doi.org/10.1111/j.1540-5915.2012.00361.x.