Weber, Ramona; Gernreich, Chris C.; Wolf, Verena



# „Sie werden eh einen Weg finden, um es zu umgehen“ – Ein führender Automobilhersteller kämpft mit Datensicherheit in der Neuproduktentwicklung

HMD Praxis der Wirtschaftsinformatik

**Provided in Cooperation with:**
Springer Nature

*Suggested Citation:* Weber, Ramona; Gernreich, Chris C.; Wolf, Verena (2021) : „Sie werden eh einen Weg finden, um es zu umgehen“ – Ein führender Automobilhersteller kämpft mit Datensicherheit in der Neuproduktentwicklung, HMD Praxis der Wirtschaftsinformatik, ISSN 2198-2775, Springer Fachmedien Wiesbaden, Wiesbaden, Vol. 59, Iss. 4, pp. 1101-1116, https://doi.org/10.1365/s40702-021-00805-0

This Version is available at:
https://hdl.handle.net/10419/287728

HMD (2022) 59:1101–1116
https://doi.org/10.1365/s40702-021-00805-0

SPEKTRUM

# „Sie werden eh einen Weg finden, um es zu umgehen" – Ein führender Automobilhersteller kämpft mit Datensicherheit in der Neuproduktentwicklung

**Ramona Weber · Chris C. Gernreich · Verena Wolf**

Eingegangen: 9. August 2021 / Angenommen: 7. Oktober 2021 / Online publiziert: 28. Oktober 2021


**Zusammenfassung** Während sich Unternehmen die Möglichkeiten der vernetzten Informations- und Kommunikationstechnologie für die gemeinsame Entwicklung neuer Produkte zunutze machen, stellen sich gleichzeitig Fragen nach dem Schutz von vertraulichen Informationen und Wissen. Um ihre ungewollte Verbreitung zu vermeiden, benötigen Unternehmen in verschiedenen Branchen klare Strategien zur Risikominimierung. Durch den aktuellen Wandel hin zur Elektromobilität herrscht in der Automobilindustrie ein harter Wettbewerb und die Gefahr von Nachahmung ist groß. Wir präsentieren eine explorative Fallstudie in einem führenden europäischen Automobilunternehmen und untersuchen das Verhalten am Arbeitsplatz und die damit verbundenen Informationssicherheit bei der Entwicklung neuer Produkte. Die Ergebnisse zeigen, dass das Bewusstsein zum Schutz von Informationen in Organisationsroutinen verwurzelt ist und dass bestehende Sicherheitsmaßnahmen eine schwache Wirkung haben. Unpraktische formale Sicherheitsrichtlinien sowie hierarchische Spannungen und Zeitdruck führen zu riskanten Verhaltensweisen der Mitarbeiter. Unsere Ergebnisse weisen auf die Bedeutung von Transparenz und Flexibilität von Wissenssicherheitsrichtlinien hin. Darüber hinaus bieten wir eine neue Perspektive auf den Wissenstransfer, indem wir die sog. Sichtbarkeitslinie für Informationen einführen und einen Sicherheitsrahmen für die Praxis vorstellen.

Ramona Weber
University of Leicester, Leicester, Großbritannien

Chris C. Gernreich (✉)
Ruhr-Universität Bochum, Bochum, Deutschland
E-Mail: chris.gernreich@rub.de

Verena Wolf
Universität Paderborn, Paderborn, Deutschland

**Schlüsselwörter** Wissensmanagement · Datensicherheit · Neuproduktentwicklung · Innovationsmanagement · Digitalisierung · Automobilindustrie

## "They'll find a way around it anyway" – A leading car manufacturer struggles with data security in new product development

**Abstract** While companies embrace opportunities for interconnected information and communication technology for a joint development of new products, issues around the protection of information and knowledge arise simultaneously. To avoid undesired information diffusion, organizations across various industries need clear risk-mitigating strategies. Due to the change toward electric mobility, the automotive industry faces fierce competition, and the threat of imitation is high. We perform an exploratory case study in a leading European automotive company, examining workplace behavior and related information security issues in new product development. The results show that perceptions of knowledge security are rooted in organizational routines and that existing security measures have a weak effect. Unpractical formal security guidelines as well as hierarchical pressure and time constraints lead to risky actions of employees. Our findings point out the importance of the transparency and flexibility of knowledge security guidelines. Furthermore, we provide a new perspective on knowledge transfer by introducing a line of visibility for information and introducing a security framework for practice.

**Keywords** Knowledge management · Data security · New product development · Innovation management · Digitalization · Automotive industry

## 1 Der Wandel als Herausforderung für Unternehmen

Profitabilität und Erfolg entstehen nicht automatisch durch Produktverkäufe, sondern resultieren aus innovativen Ideen, bewusstem Wissens- und Informationsmanagement (Alavi und Leidner 2001; Annansingh 2012; Teece 2007; Whitman und Mattord 2015). Insbesondere gemeinsame Innovationsaktivitäten sind eine vielversprechende Quelle für Innovationen (Chesbrough et al. 2006). Die Digitalisierung ermöglicht es interorganisationalen Projektpartnern, ihre digitalen Prototypen virtuell zu entwickeln und zu testen (Schwab 2017). Gleichzeitig ermöglicht die Digitalisierung von Geschäftsprozessen die Nutzung von Technologie in einem breiten sozialen und institutionellen Kontext (Tilson et al. 2010). Obwohl die Forschung zur Informationssicherheit schon vor einiger Zeit als zu techniklastig kritisiert wurde (z. B. Ilvonen et al., 2015a; Padyab et al., 2014), wird das Verhalten von Menschen dabei erst langsam verstanden (z. B. Klipper 2020, Reinheimer und Weber 2020). Zudem ist das Thema Informationssicherheit in der deutschsprachigen Literatur und somit auch in der Diskussion bisher kaum präsent (Weber 2020), dabei ist das Thema in internationaler Literatur schon länger von hoher Relevanz (z. B. Gordon und Loeb 2002; Bulgurcu et al. 2010; Moody et al. 2018). Informationssicherheit umfasst mehr als rein technische Lösungen; sie berücksichtigt andere potenzielle Risiken,

die durch menschliches Verhalten entstehen, das in Geschäftsprozessen vorgegeben und in Organisationsroutinen – sich iterativ verändernde und wahrnehmbare Verhaltensmuster verschiedener Akteure (Feldman et al. 2016) – manifestiert ist (Desouza 2006; Ilvonen et al. 2015b). Aufgrund dieser Entwicklung sind die wertvollen Wissensbestände einer Organisation zunehmend anfällig für Sicherheitsverletzungen (IBM Security und Ponemon Institute 2017; Schwab 2017), wie zuletzt das Bekanntwerden tausender Kundendaten von VW und Audi in einem Hackerforum zeigte (Tremmel 2021). Infolgedessen gehören Fragen der Informationssicherheit zu den größten Bedrohungen für Organisationen heutzutage (Whitman und Mattord 2015).

Die Automobilindustrie ist wissensintensiv und wettbewerbsintensiv, so dass strenge Maßnahmen zur Sicherung des geistigen Eigentums entscheidend sind (Jordan und Jones 1997). Wenn eine Vernachlässigung solcher Sicherungsmaßnahmen zum Abfluss von wettbewerbsrelevantem Wissen in Richtung von Wettbewerbern führt, können mühsam erarbeitete Wettbewerbsvorteile schwinden. Nach den Turbulenzen durch den Skandal um manipulierte Abgaswerte hat sich die europäische Automobilindustrie auf umweltfreundliche Lösungen umorientiert (Gracia und Paz 2017). Dies beinhaltet einen Übergang von Verbrennungsmotoren zu Elektro- und Wasserstofffahrzeugen. In diesem Zusammenhang sammeln europäische Automobilunternehmen neues Wissen, um mit der von der asiatischen Automobilindustrie entwickelten Elektrofahrzeugtechnologie Schritt zu halten (Fredriksson et al. 2018). Gleichzeitig sind die europäischen Automobilunternehmen sehr daran interessiert, ihr geistiges Eigentum zu schützen, da ihre Produktionstechnologie als führend in der Automobilproduktion gilt (Günther et al. 2015). Bisher wurde Informationssicherheit allerdings kaum in Unternehmensbereichen mit speziellen Anforderungen erforscht (Kraft und Stöwer 2017). Daher ist die Entwicklung neuer Produkte innerhalb der europäischen Automobilindustrie ein interessanter Kontext, in dem untersucht werden kann, wie Organisationen den Wissenserwerb und -austausch ausbalancieren (Canonico et al. 2018; Gonzalez 2017; Darmawan und Suzianti 2020) und gleichzeitig die Kontrolle über vertrauliche Informationen behalten (Jennex und Durcikova 2013). Daher zielen wir darauf ab, die folgende Forschungsfrage zu beantworten:

*Wie wird Informationssicherheit durch Organisationsroutinen von Mitarbeitern in der Neuproduktentwicklung der Automobilindustrie beeinflusst?*

Zunächst werden das Konzept des Wissens und die Bedeutung der Wissenssicherheit in neuen Produktentwicklungsprojekten erläutert. Dann wird das Forschungsdesign begründet, gefolgt von einer Beschreibung der Fallstudie und des methodischen Ansatzes zur Datenanalyse. Um diese Forschungsfrage zu beantworten, führen wir eine Fallstudie bei einem europäischen Automobilhersteller durch und sammeln mehrere Datenquellen, im Kern handelt es sich um zehn Interviews mit Schlüsselinformanten aus der Prototyp-Abteilung. Wir leiten vier Thesen für die Informationssicherheit ab, die zukünftige Forschung und Praktiker in wettbewerbsintensiven Branchen wie der Automobilindustrie leiten können (Kuhnert et al. 2018). Zusammenfassend stellen wir auf Basis der Thesen das POWA-Framework dar, das Organisationen zur Ausrichtung ihrer Wissensmanagementstrategie nutzen können.

## 2 Grundlagen

### 2.1 Informationssicherheit

Informationen sind eine wichtige operante Ressource (Vargo und Lusch 2004), die es Organisationen ermöglicht, einen einzigartigen Wettbewerbsvorteil zu erzielen (Alavi und Leidner 2001; Davenport und Prusak 1998). Organisationen nutzen Informationen dazu, wissensbezogenen Vermögenswerte zu generieren (Coakes 2004). Wissen wird in den Organisationsroutinen von Mitarbeitern gespeichert, die in Interaktionsmuster mit anderen Mitarbeitern eingebunden sind. Dabei teilen die Mitarbeiter Informationen und generieren wiederum neue Werte (Feldman 2000; von Hippel 2007). Auf diese Weise wird organisationales Wissen durch Sozialisation und Interaktion, d. h. durch gemeinsames Denken und Kommunizieren, geschaffen und entwickelt (Edmondson 2002; Feldman 2000).

Während sich das Wissensmanagement auf die Generierung von Werten durch den Austausch von Wissen konzentriert (Edmondson 2002), ist der Zweck der Informationssicherheit die Sicherstellung und der Schutz der Vertraulichkeit (Zugriff nur durch autorisierte Personen), der Integrität (Transparenz über alle Datenänderungen) und der Verfügbarkeit (jederzeitiger Zugriff auf Daten und Systeme) von Informationen (Taylor 2013). Maßnahmen zur Schaffung von Informationssicherheit zielen darauf ab, beim Aufbau von Informations- und Kommunikationssysteme potenzielle Risiken zu berücksichtigen, die sowohl IT- als auch nicht-IT-bezogen sind. Allerdings zeigen sich viele Risiko-Analysemethoden für die Informationssicherheit sehr detailliert und professionalisiert (Kardel 2011; Johannsen und Kant 2020) was ihre Praktikabilität reduziert.

### 2.2 Der Faktor Mensch

Ein zentrales Element der Wissenssicherheit ist der sogenannte menschliche Faktor (Desouza 2006; Ilvonen et al. 2015b). Etwa die Hälfte aller Sicherheitsverstöße geschieht versehentlich (EY 2017). Verletzungen der Wissenssicherheit treten auf, wenn verschiedene Arten des Wissensaustauschs verwendet werden, wie z. B. schriftliche Dokumente, persönliche Interaktionen, organisatorische Kommunikation oder in Communities of Practice (Yi 2009). Die Kommunikation über digitale Kanäle ist anfällig für Fehler und Bedrohungen hinsichtlich des Abflusses von kritischem Wissen und Informationen (Annansingh 2012). Desouza (2006, S. XII) betont die Tatsache, dass „Wissen kein Produkt ist; Wissen ist flüssig, dynamisch und mobiler als jedes andere physische Produkt." Daher stellt das Verhalten menschlicher Akteure, wie Mitarbeiter, Geschäftspartner und andere Stakeholder, und ihr Umgang mit sensiblen Informationen und Wissen ein erhebliches Risiko für Wissensverlust dar (IBM Security und Ponemon Institute 2017). Verschärft wird dieses Problem durch die immer stärkere Nutzung externer Informationsrepositorien (Alavi und Leidner 2001), wie z. B. mobile Geräte (Santos und Ali 2012) oder Social-Media-Kommunikationsplattformen (Ahmed et al. 2019). Die Nutzung von externen Ressourcen führt zu einer geringeren organisatorischen Kontrolle über Mitarbeiter und Wissen. Insbesondere der Inhalt dessen, was geteilt wird, die Menge des geteilten Inhalts

und die Personen, mit denen der Inhalt geteilt wird, sind davon betroffen (Väyrynen et al. 2013). Wenn Geräte sowohl für berufliche als auch für private Zwecke genutzt werden, verschwimmen die Grenzen organisationaler Systeme, was die Wissenskontrolle noch schwieriger macht (Väyrynen et al. 2013). Die Vernachlässigung von Richtlinien zur Wissenssicherheit oder ein falscher Umgang mit Informationen kann dann zu einer unbeabsichtigten Verbreitung von Ideen an unvorhergesehene Empfänger führen (Cheung et al. 2012).

### 2.3 Wissen in der Neuproduktentwicklung

Der Automobilsektor hat sich in den letzten Jahrzehnten durch neuartige technologische Entwicklungen disruptiv verändert (Mohr et al. 2016). Diese Entwicklungen erfordern von den Unternehmen der Branche, sich neues Wissen anzueignen und eine immer breitere Wissensbasis zu pflegen, um sich im harten internationalen Wettbewerb zu behaupten (Demirkan und Spohrer 2015), bspw. die Entwicklung eigener Betriebssysteme oder spezialisierter Chip-Architekturen durch die Volkswagen AG. Die Integration von technischen Spezifikationen in (digitale) Produkte sowie die kritische Prüfung und Bewertung neuer Produkte, wie im Rahmen des Wandels zur Elektromobilität, sind im Prozess der Neuproduktentwicklung unerlässlich. Die Ergebnisse der Bewertung werden für zukünftige Anpassungen und Verbesserungen des Produkts und seines Produktionsprozesses aggregiert und formalisiert (Cooper 2001). Weitere Verbesserungen können durch das kontinuierliche Sammeln von Informationen über die Produktnutzung und damit verbundene Produkttrends erreicht werden (Kuhnert et al. 2018).

Eine weitere Quelle, durch die neues Wissen erworben wird, ist die gemeinsame Entwicklung von Produkten mit Lieferanten und anderen Geschäftspartnern, z. B. für autonome Fahrzeuge (Potter und Graham 2019). Die Möglichkeit zur Zusammenarbeit wird durch digitale Technologien erweitert, die neue Formen der gleichzeitigen Zusammenarbeit und eine effizientere Verarbeitung sensibler konstruktions- und produktionsbezogener Daten ermöglichen. Diese Technologie bietet dann eine Infrastruktur für die simulationsbasierte kollaborative Entwicklung neuer Produkte (Xu et al. 2012). Der Austausch vertraulicher Informationen mit Dritten, wie z. B. Lieferanten, Technologieanbietern, einzelnen Beratern oder akademischen Einrichtungen, ist für die Entwicklung neuer Produkte unerlässlich (von Hippel 2007). Mitarbeiter müssen innerhalb und über die verschiedenen Phasen der Neuproduktentwicklung hinweg Wissen erwerben und teilen (Watson und Hewett 2006).

## 3 Methodisches Vorgehen

Um das Phänomen der Informationssicherheit in der Neuproduktentwicklung in seinem realen Kontext zu untersuchen, wurde eine explorative Fallstudie nach Yin (2018) mit einem induktiven Vorgehen bei einem führenden europäischen Automobilunternehmen durchgeführt. Die Fallstudie bietet tiefe Einblicke in die Informationssicherheit eines Unternehmens in der Automobilbranche, indem sie die Verflechtung von Technologie, Prozessen und menschlichen Faktoren beleuchtet (Rauch

et al. 2014). Das Unternehmen beschäftigt ca. 5000 Mitarbeiter und ist einer der Qualitätsführer der Automobilbranche. Es ist gut im Markt etabliert und strebt in seiner Branche eine führende Position in Bezug auf Qualität und Technologie an. Diese Strategie erfordert umfangreiche und kontinuierliche Aktivitäten im Bereich der Neuproduktentwicklung. Da das Unternehmen durch seine angestrebte Marktführerschaft neue und komplexe Produkte entwickeln muss, stimmt es die Produktanforderungen regelmäßig mit anderen internationalen Lieferanten während des gesamten Neuproduktentwicklungsprozesses ab.

Im Rahmen der Fallstudie führten wir über einen Zeitraum von sechs Monaten eine Datenerhebung innerhalb des Unternehmens durch. Diese Datenerhebung umfasste Beobachtungen und halbstrukturierte Interviews mit zehn Experten aus der Prototyp-Abteilung der Organisation, um die Erfahrungen der Befragten mit Wissenssicherheit zu beleuchten (Gilbert und Stoneman 2016). Außerdem fand eine Datentriangulation statt, welche die Analyse von internen Dokumenten und Feldnotizen sowie von Kontextinformationen durch Beobachtungen beinhaltet. Die Informanten üben entweder Kernfunktionen aus, die sich mit digitalem Design, der Entwicklung von Prototypen und der Produktentwicklung befassen, oder unterstützende Funktionen im Innovationsmanagement, Virtual-Reality-Management und Prozess-Engineering (siehe Tab. 1).

Insgesamt dauerten die Interviews acht Stunden und 27 min (M = 50,7 min). Um sicherzustellen, dass die befragten Informanten einen substanziellen Beitrag zur Forschungsfrage leisten (Gilbert und Stoneman 2016), begannen wir mit der Befragung von Informanten in der Prototyp-Abteilung und sichteten anschließend das Organigramm, um weitere Informanten anhand ihrer Positionen und Verantwortlichkeiten auszuwählen, um eine theoretische Sättigung zu erreichen. Allen Informanten wurde strengste Vertraulichkeit zugesichert, einschließlich ihres Arbeitgebers. Dies ermöglichte es uns, nach sehr sensiblen Informationen zu fragen, wie z. B. nach selbstverschuldeten Sicherheitsverletzungen.

Alle gesammelten Daten wurden trianguliert und nach den Richtlinien von Mayring (2014) für die qualitative Inhaltsanalyse analysiert. Ein induktiver Ansatz zur Theorieentwicklung leitete die Fallstudie. Durch dieses Vorgehen konnte ein tiefgehendes Verständnis des Phänomens im Kontext gewonnen werden, welches die

**Tab. 1** Interviewstichprobe

| Informant | Position | Betriebszugehörigkeit (Jahre) |
|---|---|---|
| A | Innovationsmanagement | 7 |
| B | Digitales Design und Prototypentwicklung | 1 |
| C | Digitales Design und Prototypentwicklung | 1 |
| D | Digitales Design und Prototypentwicklung | 12 |
| E | Produktentwicklung | 8 |
| F | Innovationsmanagement | 3 |
| G | Digitales Design und Prototypentwicklung | 15 |
| H | Produktentwicklung | 2 |
| I | Produktentwicklung | 1 |
| J | Virtual-Reality-Management | 2 |

Entwicklung neuer theoretische Erkenntnisse leitete (Gilbert und Stoneman 2016). Um dies zu erreichen, wurden die Aussagen auf die Kernaussagen zusammengefasst, um diese anschließend zu kodieren (Gilbert und Stoneman 2016; Mayring 2014). Dieses Vorgehen ermöglichte es uns, einen klaren Überblick über die Daten zu erhalten, ohne die ursprünglichen Daten zu verzerren (Mayring 2014).

## 4 Ergebnisse und Diskussion

### 4.1 Sichtbarkeit für interne und externe Personen

Der untersuchte Fall zeigt, dass die Zusammenarbeit mit externen Dritten häufig die Offenlegung vertraulicher Informationen erfordert, was voraussetzt, dass sich beide Partner gegenseitig vertrauen. Dazu gehören 2D- und 3D-Produktdesigndaten, technische Spezifikationen, Bilder von Prototypen und Beschreibungen von physischen Teilen. Virtual Reality bietet den Informanten in ihrem Unternehmen die Möglichkeit, Prototypen gemeinsam mit mehreren Personen in Partnerunternehmen zu testen. Daher werden die virtuellen Daten über ein Datenaustauschsystem gemeinsam genutzt. Die befragten Mitarbeiter erklärten, dass eine Geheimhaltungsvereinbarung von Personen beim Partnerunternehmen unterzeichnet wird, bevor die Informationen freigegeben werden. Personen, die auf eine Virtual-Reality-Software zugreifen, übermitteln in einer Sitzung Positionsdaten, was den Managern die Kontrolle über die Zielgruppe gibt, welche an der Sitzung teilnimmt. Einige Informanten äußerten Bedenken, dass der Standort (d. h. die physische Umgebung) der Person, die an der Sitzung teilnimmt, sicher sein muss. Dies ist insbesondere dann von hoher Relevanz, wenn eine Virtual-Reality-Sitzung auf einem Bildschirm in einer öffentlichen Umgebung angezeigt wird. In einer solchen Situation könnten die Inhalte von Unbefugten eingesehen werden, die sich außerhalb der Sichtweite der verantwortlichen Personen befinden oder die Umgebung der Endgeräte keinen ausreichenden Sicherheits- und Zugangskontrollen unterliegen (Sowa 2008).

Wie in Abb. 1 dargestellt, verändert sich der Wissenszugang durch die Zusammenarbeit mit Dritten. Organisationen können den Fluss vertraulicher Informationen und die Ansammlung von Wissen innerhalb der eigenen Organisationsgrenzen kontrollieren, indem sie Richtlinien etablieren und Schulungen durchführen. Auf diese Weise bleiben vertrauliche Informationen unbefugten Dritten verborgen (dargestellt durch die Sichtbarkeitslinie). Durch das Teilen von Wissen für die Zusammenarbeit mit externen Personen und Partnerunternehmen, wie Zulieferern verschiebt sich die Sichtbarkeitslinie von einem internen Adressatenkreis in Richtung Dritte, d. h. die Dritten können somit leicht auf sensible Unternehmensinformationen zugreifen. Die Informanten der Fallstudie haben die Sorge geäußert, dass, sobald Dritte Zugang zu Daten haben, keine weitere Kontrolle mehr besteht. Infolgedessen können Dritte diese Informationen für ihre eigenen Zwecke nutzen oder sogar an andere Unternehmen verkaufen. Die interorganisationale Zusammenarbeit mit Lieferanten und anderen Geschäftspartnern kann ebenfalls problematisch sein, da Dritte erworbenes Wissen verbreiten, wenn sie für Wettbewerber in der Branche arbeiten (Gernreich et al. 2018). Dies kann sogar ohne eine negative Absicht geschehen, da sowohl in-

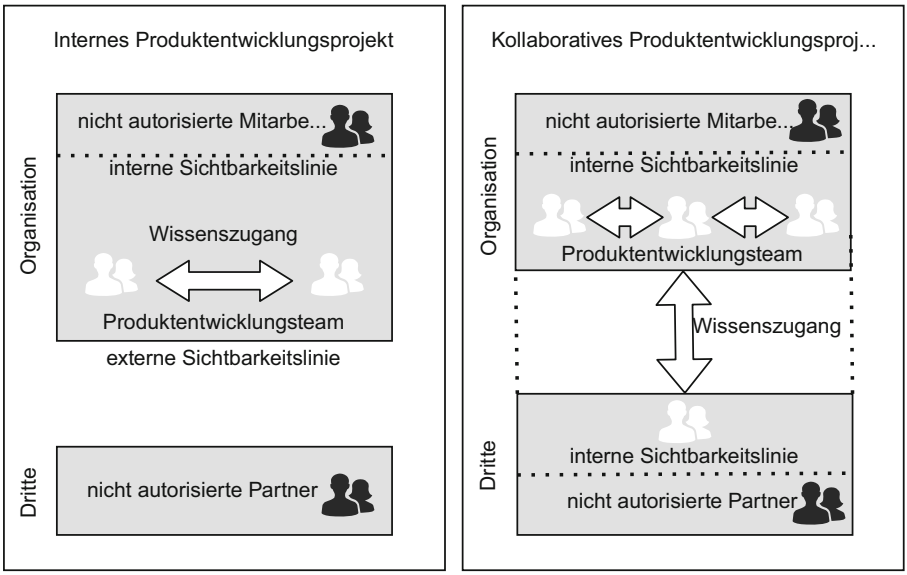



**Abb. 1** Sichtbarkeit und Wissenszugang mit der Sichtbarkeitslinie

terne Mitarbeiter als auch externe Personen in Partnerunternehmen in verschiedenen europäischen Ländern aufgrund kultureller und rechtlicher Unterschiede Informationssicherheit unterschiedlich auslegen (Custers et al. 2018).

Allerdings lässt sich feststellen, dass die Sicherheitsrisiken durch die Verschiebung der Sichtbarkeitslinie Richtung Dritte je nach wirtschaftlicher Abhängigkeit variieren. Die Sichtbarkeitslinie von vertraulichem Wissen verschiebt sich ggf. sogar zu Organisationen in anderen Rechtsräumen, wenn Lieferanten mit diesen zusammenarbeiten. Die verschobene Sichtbarkeitslinie induziert eine Wissensdiffusion zu den Vertragspartnern der Zulieferer.

***These 1:*** *Informationssicherheitsmaßnahmen sind unzureichend in Bezug auf die Diffusion von Informationen sobald sie bei externen Personen in Partnerunternehmen bzw. Dritten liegen.*

### 4.2 Prägung der Sicherheitskultur durch die Organisationsroutinen

Die Interviews zeigen, dass es bei den Informanten ein unterschiedliches Sicherheitsbewusstsein im Umgang mit vertraulichen Informationen und Wissen gibt. Über die Berechtigungsebene der Projektpartner und deren Berechtigung, vertrauliche Informationen zu erhalten, konnten bspw. mehrere Informanten nur Vermutungen anstellen, da die Berechtigungsebenen der Personen in Partnerunternehmen nicht zentral definiert oder bestätigt wurden. Informant E (Produktentwicklung) gab an, dass er sich keine Sorgen um die Informationssicherheit macht, wenn er Informationen innerhalb der Organisation weitergibt. Im Gegensatz dazu prüft Informant G (Digitales Design und Prototypentwicklung) immer, wer die Informationen anfordert,

warum und was diese Person damit zu tun beabsichtigt. Informant G ist in einer viel früheren Phase des Produktentwicklungsprozesses involviert und verlangt, dass die Informationen noch sicherer aufbewahrt werden.

Die meisten Informanten sind der Meinung, dass Dokumente mit Vertraulichkeitseinstufungen meist nur für eine bestimmte Zielgruppe relevant sind. Darüber hinaus wird Vertraulichkeit als prozessimmanent angesehen, wie Informant B (Digitales Design und Prototypenentwicklung) erklärt. Er findet, dass der Entwicklungsprozess mit seinen Rollen und Richtlinien alle Eventualitäten abdeckt. Auf diese Weise wird Vertraulichkeit aufgrund der formalen Rollen der Mitarbeiter innerhalb der Forschungs- und Entwicklungsabteilung als natürlich angesehen. Die Organisation vertraut den Mitarbeitern und einige der Informanten gehen davon aus, dass Vertraulichkeit für alle beteiligten Mitarbeiter gleichermaßen wichtig ist. Mehrere Informanten gehen davon aus, dass Personen innerhalb der gleichen Organisation im Allgemeinen an die gleichen Verhaltensregeln und ethischen Grundsätze gebunden sind, welche in ihren Organisationsroutinen verankert sind. Zusätzliche Sicherheitsvorkehrungen werden nicht getroffen, da die Mitarbeiter ihren Kollegen, ihrer Organisation und den IT-Systemen der Zulieferer bei der Handhabung und Weitergabe vertraulicher Informationen vertrauen. Allerdings erklärten manche Informanten, dass sie Arbeitsaufgaben unter hohem Zeitdruck zu erledigen, wie Informant G hervorhob: *„Unser Arbeitspensum nimmt ständig zu, aber wir haben immer weniger Zeit, um es zu erledigen.“*. Dies führt oft zu Situationen, in denen Wissen auf unkonventionelle Weise geteilt wird, wie z. B. über WhatsApp und zunehmend über soziale Medien (Ahmed et al. 2019).

Zusammenfassend wird festgestellt, dass Informanten, die in früheren Phasen des Produktentwicklungsprozesses arbeiten, ein größeres Bewusstsein für die Bedeutung von Vertraulichkeit haben als Informanten, die in späteren Phasen arbeiten. Mit Ausnahme von Informant G vertrauten alle Informanten den Dokumenten und Kommunikationspartnern, mit denen sie in Kontakt kamen, ohne deren Vertraulichkeitsgrad oder Berechtigung zum Zugriff auf bestimmte Informationen und Wissen zu prüfen.

***These 2:*** *Informationssicherheit wird durch die gelebten Organisationsroutinen der Mitarbeiter verankert.*

### 4.3 Workarounds zur Erreichung von Unternehmenszielen

Die meisten Informanten gaben an, dass der Großteil der Kommunikation und des Informationsaustauschs über E-Mail, Telefon, persönliche Treffen, Telefonkonferenzen, webbasierte Kollaborationsplattformen oder Datenaustauschsysteme erfolgt. Obwohl Studien vor Jahren zeigten, dass Mitarbeiter Online-Kollaborationstools auch dann nutzen, wenn es offensichtliche Sicherheitsprobleme gibt (Jarvenpaa und Majchrzak 2010), tauschen die Interviewpartner Informationen mit Dritten hauptsächlich über unverschlüsselte E-Mails oder Datenaustauschsysteme aus. Arbeit im Home-Office ermöglicht es den Informanten auch, ihre von der Arbeit zur Verfügung gestellten Laptops mitzunehmen und zu Hause, beim Lieferanten oder auf Geschäftsreisen zu nutzen. Darüber hinaus werden auch Ausdrucke und Datenspeicher,

wie z. B. externe Festplatten, regelmäßig aus dienstlichen Gründen meist ungefragt mitgenommen oder als Backups verwendet. Die Genehmigung des Vorgesetzten für die Nutzung eines USB-Sticks einzuholen, ist zu zeitaufwändig, wie Informant G berichtet:

> *Wenn das tägliche Praxis wäre, würden die Leute einfach mit USB-Sticks herumlaufen, was ich nicht gerne mache, weil ich erst sehen müsste, dass der Vorgesetzte da ist, um es abzusegnen [was deutlich mehr Zeit kosten und den Arbeitsablauf ins Stocken bringen würde] – selbst wenn die Leute die Informationen sofort brauchen – und ich müsste vielleicht wochenlang warten, um die Unterschrift des Vorgesetzten zu bekommen.*

Die befragten Informanten nutzen mobile Endgeräte für ihre Arbeit, was eine weitere Quelle für die unkontrollierte Offenlegung vertraulicher Informationen darstellt (Disterer und Kleiner 2014). Fremde Anwendungen, die auf dem Gerät eines Mitarbeiters installiert sind, können unbefugt auf vertrauliche Informationen zugreifen, sogar dann, wenn der Zugriff auf diese Informationen nicht explizit gewährt wurde (Kleiner und Disterer 2015).

Informant J machte besonders deutlich, dass *„der Fokus von der Sicherheit vor Ort, wie dem Sperren des Zugangs zu bestimmten Bereichen, losen Papieren und physischen Geräten, auf die Sicherheit zur Vermeidung der Offenlegung von Informationen über das Internet verlagern muss.“*. Fast alle Informanten erklärten, dass es immer wieder zu Zeitdruck durch das Management und in Bezug auf Projektpläne kommt, was den Einsatz von Schatten-IT zur Folge hat. Die digitale Produktentwicklung ermöglicht es Unternehmen nicht nur Kosten zu senken und Produkte schneller zu entwickeln, sondern auch Entscheidungen früher zu treffen und den Produktlebenszyklus zu verkürzen. Die Informanten berichten über das Fehlen von Möglichkeiten, Informationen einfach, schnell und *sicher* zu teilen. Infolgedessen sind die Informanten auf alternative Dienste angewiesen, um Daten auszutauschen, um die schnelle Entwicklung eines Produkts nicht zu gefährden. Um die Sicherheit im Umgang mit vertraulichen Daten zu gewährleisten, ist ein anwendbares, nachvollziehbares und sicheres Datenmanagementsystem mit transparenten Regeln und Prozessen entscheidend. *„Andernfalls werden die Leute eh einen Weg finden, einen nicht abgesicherten Prozess zu umgehen“*, so Informant A.

**These 3:** *Vom Management initiierte Sicherheitsrichtlinien können zu Workarounds führen, um Organisationsziele zu erreichen.*

### 4.4 Erzeugung von Aufmerksamkeit für sicherheitsrelevante Daten und Information

Die Interviews zeigen deutlich, dass es sowohl bei der sicheren Kommunikation als auch beim Sicherheitsbewusstsein an formalen Sicherheitsprozessen mangelt. Informant C (Digitales Design und Prototypentwicklung) konstatierte, dass es kaum formale schriftliche Sicherheitsprozesse speziell für den sensiblen Bereich der Entwicklung neuer Produkte gebe. Außerdem seien die Sicherheitsmaßnahmen nur allgemeines Wissen und nicht rollenspezifisch, wie sie sein sollten (Rechberg und

Syed 2014). Die Sicherheitsmaßnahmen müssen aufgrund der zunehmenden Digitalisierung ergänzt werden; die Informanten betonten jedoch die konträre Realität der uneinheitlichen Sicherheit und Prozesse in den verschiedenen Phasen von Neuproduktentwicklungsprojekten. Mehrere Informanten wünschten sich bequemere und praktikablere Sicherheitsrichtlinien sowie Schulungen zum sicheren Umgang mit vertraulichen Informationen innerhalb der Organisation, da sie in ihrem Alltag eher nur Vermutungen darüber treffen, wie vertrauenswürdig der Kommunikationspartner ist. Nur Informant D (Digitales Design und Prototypentwicklung) gab an, dass seine Rollen, Verantwortlichkeiten und Partner zu Beginn eines Projekts definiert würden. Bei diesem Vorgehen wird der Zugang zu Systemen und Daten kontrolliert und die Beteiligten wissen, an wen sie Daten senden können und an wen nicht. Die anderen Informanten gaben an, dass sie weder unterrichtet noch grundsätzlich geschult wurden, welche Informationen und welches Wissen vertraulich sind und wie sie damit umgehen sollen. Da alle Informanten im gleichen Unternehmen arbeiten, ist diese Uneinigkeit ein deutlicher Hinweis darauf, dass entweder keine einheitlichen Sicherheitsrichtlinien vorliegen oder das Wissen der Informanten diesbezüglich nicht nachhaltig gesichert wurde, bspw. durch die Dokumentation in einer Kommunikationsmatrix (Project Management Institute 2013). Allerdings sollte betont werden, dass auch ausgeklügelte Kontrollen umgangen werden bzw. nicht einhundertprozentig sicher sein können. Grobe Fahrlässigkeit und Vorsatz zeigen sich häufig in menschlichem Verhalten.

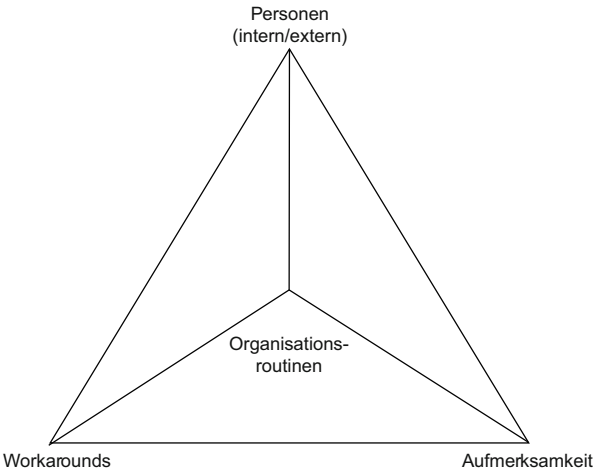
Einige Informanten gaben auch an, dass ihre Sorge um die Vertraulichkeit davon abhängt, ob sich die Informationen auf die Gegenwart oder die Zukunft beziehen. Diese Informanten behandeln vertrauliche Informationen anders, wenn sich die Informationen auf eine zukünftige Phase des Projekts beziehen. Die Informanten stufen Informationen über zukünftige Projekte als vertraulich und Informationen über ein laufendes Projekt als weniger vertraulich ein. Beispielsweise stufen die Informanten der Produktentwicklung Informationen über das zur Zeit der Interviews aktuelle konzeptionelle Design nicht eindeutig als vertraulicher ein als Informationen über den zukünftigen Produktionsprozess oder die Markteinführung.

***These 4:*** *Sicherheitsrichtlinien müssen kommuniziert werden und für die Mitarbeiter transparent sein, damit die Aufmerksamkeit der Mitarbeiter für sensible Daten gewährleistet werden kann.*

## 5 Zusammenfassung

Die vorliegenden Ergebnisse legen nahe, dass selbst große Organisationen mit der Informationssicherheit in der Neuproduktentwicklung in einer der weltweit fortschrittlichsten Industrien zu kämpfen haben. Die vier vorgestellten Thesen fassen wir im Folgenden als das POWA-Framework zusammen (P = Personen, O = Organisationsroutinen, W = Workarounds, A = Aufmerksamkeit), das die Eckpfeiler der Informationssicherheit für die hochkollaborative und stark digitalisierte Neuproduktentwicklung in der Automobilindustrie abbildet (siehe Abb. 2). Dabei zeigt sich, dass die Informationssicherheit als ein zentrales Konstrukt auf Perso-

**Abb. 2** POWA-Framework




nenebene ist, welche durch die Aufmerksamkeit der betreffenden Personen, die Etablierung von Organisationsroutinen sowie die Ausführung von Workarounds geprägt wird. Das Framework kann eine erste Hilfe sein, um systematisch bestehende Unzulänglichkeiten zu identifizieren.

Erstens verschiebt sich durch die Bereitstellung oder Weitergabe von Informationen an interne und externe Personen (P) die Sichtbarkeitslinie, welche mit einem zu bewertenden Risiko der unkontrollierten Weitergabe verbunden ist. Insbesondere bei der Weitergabe an externe Personen in z. B. Partnerunternehmen stellt der damit verbundene Kontrollverlust ein kritischer Aspekt dar, der von Sicherheitsrisikomanagern berücksichtigt werden muss. Zweitens müssen die Organisationroutinen (O) evaluiert und kontrolliert werden. Verantwortliche müssen Rollen im Neuproduktentwicklungsprozess definieren und formale Anhaltspunkte für die Interaktion zwischen diesen Rollen bieten. Die Aufklärung der Mitarbeiter über rollenspezifische Sicherheitsanforderungen während der Produktentwicklung kann bei den Mitarbeitern ein Verständnis dafür schaffen, dass sie sorgfältig und vorausschauend handeln müssen. Drittens müssen die Richtlinien und Vorschriften für das Wissensmanagement transparent, den Mitarbeitern bewusst und leicht anwendbar sein. Sie müssen so klar sein, dass ein Verstoß oder Nichteinhalten dieser Richtlinien Aufmerksamkeit (A) erzeugt und entsprechende Maßnahmen ergriffen werden. Dazu können Organisationen Risikobewertungen durchführen, indem sie ein Inventar von Informationswerten erstellen, wie von Padyab et al. (2014) vorgeschlagen. Neben der Identifizierung von Informationswerten und -entitäten hilft es, die Abteilungen einer Organisation zu bestimmen, die für den Wertschöpfungsprozess relevant sind. Viertens muss das Sicherheitsmanagement den Mitarbeitern die Flexibilität geben, schnell auf Informationsanfragen zu reagieren und das Innovationspotenzial von Workarounds (W) zu nutzen. Es hat sich gezeigt, dass diese Verletzungen der Informationssicherheit dann auftreten, wenn die Mitarbeiter nicht die Zeit haben, die Sicherheitsanweisungen zu befolgen. Solche Abkürzungen können aber auch positiv sein, da sie Verbesserungsmöglichkeiten aufzeigen, z. B. Ideen für eine bessere Infrastruktur zum sicheren Informationsaustausch unter Zeitdruck.

Diese Fallstudie bietet spannende Einblicke in ein aktuelles und sensibles Themengebiet. Informationssicherheit in Großunternehmen ist ein streng vertrauliches Thema. Unsere Ergebnisse unterstreichen den Bedarf an weiterer Forschung. Zukünftige Forschung kann diese Ergebnisse erweitern, indem sie Muster des Wissenstransfers entwickelt, die sich aus dem Verhalten von Mitarbeitern und externen Partnern ergeben. Insbesondere das Zusammenspiel zwischen Informationssicherheits-Risikomanagement und Sicherheitskultur scheint vielversprechend und kann Erkenntnisse darüber liefern, wie die Anzahl der Sicherheitsverletzungen aufgrund von hierarchischem Druck reduziert werden kann.

Obwohl diese Untersuchung sorgfältig durchgeführt wurde, unterliegt sie einigen Limitationen. Da es sich um eine Einzelfallstudie handelt, sind die Ergebnisse in hohem Maße von den Kontext- und Umweltfaktoren abhängig, mit denen die Organisation konfrontiert ist. Daher können die Ergebnisse niemals den Anspruch erheben, repräsentativ und verallgemeinerbar für andere Organisationen zu sein, die in der gleichen Branche und von ähnlicher Größe tätig sind. Es muss berücksichtigt werden, dass zeitliche Beschränkungen sowie der Effekt des sozialen Drucks die Antworten der Informanten stark beeinflussen können.

**Funding** Open Access funding enabled and organized by Projekt DEAL.



## Literatur

Ahmed YA, Ahmad MN, Ahmad N, Zakaria NH (2019) Social media for knowledge-sharing: a systematic literature review. Telemat Inform 37:72–112. https://doi.org/10.1016/j.tele.2018.01.015

Alavi M, Leidner DE (2001) Review: knowledge management and knowledge management systems: conceptual foundations and research issues. MISQ 25:107. https://doi.org/10.2307/3250961

Annansingh F (2012) Exploring the risks of knowledge leakage: an information systems case study approach. In: Hou HT (Hrsg) New research on knowledge management models and methods. InTech, https://doi.org/10.5772/32297

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MISQ 34(3):523–548. https://doi.org/10.2307/25750690

Canonico P, Consiglio S, De Nito E, Esposito V, Pezzillo Iacono M (2018) Dealing with knowledge in a product development setting: an empirical analysis in the automotive industry. Knowl Manag Res Pract 16(1):126–133. https://doi.org/10.1080/14778238.2018.1428068

Chesbrough HW, Vanhaverbeke W, West J (2006) Open innovation: researching a new paradigm. Oxford University Press, Oxford; New York

Cheung CF, Ma R, Wong WY, Tse YL (2012) Development of an organizational knowledge capabilities assessment (OKCA) method for innovative technology enterprises. Presented at the International Conference on Innovation, Management and Technology (ICIMT 2012), Zurich, S 54–65
Coakes E (2004) Knowledge management—A primer. Commun Assoc Inf Syst 14:406–489
Cooper RG (2001) Winning at new products: accelerating the process from idea to launch, 3. Aufl. Perseus Pub, Cambridge
Custers B, Dechesne F, Sears AM, Tani T, van der Hof S (2018) A comparison of data protection legislation and policies across the EU. Comput Law Secur Rev 34:234–243. https://doi.org/10.1016/j.clsr.2017.09.001
Darmawan TS, Suzianti A (2020) Knowledge management framework in new product development projects of automotive industries. In: Proceedings of the 3rd Asia Pacific Conference on Research in Industrial and Systems Engineering, S 25–29 https://doi.org/10.1145/3400934.3400941
Davenport TH, Prusak L (1998) Working knowledge: how organizations manage what they know. Harvard Business School Press, Boston
Demirkan H, Spohrer J (2015) T-shaped innovators: identifying the right talent to support service innovation. Res Technol Manag 58:12–15. https://doi.org/10.5437/08956308X5805007
Desouza KC (2006) Knowledge security: an interesting research space. J Inf Sci Technol 3:1–7
Disterer G, Kleiner C (2014) Compliance von mobilen Endgeräten. HMD 51:307–318. https://doi.org/10.1365/s40702-014-0044-x
Edmondson AC (2002) The local and variegated nature of learning in organizations: a group-level perspective. Organ Sci 13:128–146. https://doi.org/10.1287/orsc.13.2.128.530
EY (2017) Cybersecurity regained: preparing to face cyber attacks. 20th Global Information Security Survey (No. 2017/2018). EYGM Limited,
Feldman MS (2000) Organizational routines as a source of continuous change. Organ Sci 11:611–629. https://doi.org/10.1287/orsc.11.6.611.12529
Feldman MS, Pentland BT, D'Adderio L, Lazaric N (2016) Beyond routines as things: introduction to the special issue on routine dynamics. Organ Sci 27:505–513. https://doi.org/10.1287/orsc.2016.1070
Fredriksson G, Roth A, Tagliapietra S, Veugelers R (2018) Is the European automotive industry ready for the global electric vehicle revolution? (No. 2018/26). Bruegel Policy Contributio, Brussels
Gernreich CC, Bartelheimer C, Wolf V, Prinz C (2018) The impact of process automation on manufacturers' long-term knowledge. In: Proceedings of the international conference on information systems (ICIS) San Francisco
Gilbert GN, Stoneman P (2016) Researching social life, 4. Aufl. SAGE, Los Angeles
Gonzalez RVD (2017) Knowledge management taxonomy in the Brazilian automotive industry. Knowl Manag Res Pract 15(3):491–505. https://doi.org/10.1057/s41275-017-0061-y
Gordon LA, Loeb MP (2002) The economics of information security investment. ACM Trans Inf Syst Secur 5(4):438–457. https://doi.org/10.1145/581271.581274
Gracia M, Paz MJ (2017) Network position, export patterns and competitiveness: evidence from the European automotive industry. Compet Change 21:132–158. https://doi.org/10.1177/1024529417692331
Günther H-O, Kannegiesser M, Autenrieb N (2015) The role of electric vehicles for supply chain sustainability in the automotive industry. J Clean Prod 90:220–233. https://doi.org/10.1016/j.jclepro.2014.11.058
von Hippel E (2007) The sources of innovation. In: Boersch C, Elschen R (Hrsg) Das Summa Summarum des Management. Gabler, Wiesbaden, S 111–120 https://doi.org/10.1007/978-3-8349-9320-5_10
IBM Security, Ponemon Institute (2017) 2017 cost of data breach study—global overview. Ponemon Institute LLC, North Traverse City
Ilvonen I, Jussila J, Karkkainen H, Paivarinta T (2015a) Knowledge security risk management in contemporary companies—toward a proactive approach. IEEE, S 3941–3950 https://doi.org/10.1109/HICSS.2015.472
Ilvonen I, Jussila JJ, Kärkkäinen H (2015b) Towards a business-driven process model for knowledge security risk management: making sense of knowledge risks. Int J Knowl Manag 11:1–18. https://doi.org/10.4018/IJKM.2015100101
Jarvenpaa SL, Majchrzak A (2010) Research commentary—vigilant interaction in knowledge collaboration: challenges of online user participation under ambivalence. Inf Syst Res 21:773–784. https://doi.org/10.1287/isre.1100.0320
Jennex ME, Durcikova A (2013) Assessing knowledge loss risk. IEEE, S 3478–3487 https://doi.org/10.1109/HICSS.2013.103

Johannsen A, Kant D (2020) IT-Governance, Risiko- und Compliance-Management (IT-GRC) – Ein Kompetenz-orientierter Ansatz für KMU. HMD 57:1058–1074. https://doi.org/10.1365/s40702-020-00625-8
Jordan J, Jones P (1997) Assessing your company's knowledge management style. Long Range Plann 30:392–398. https://doi.org/10.1016/S0024-6301(97)90254-5
Kardel D (2011) IT-Sicherheitsmanagement in KMU. HMD 48:44–51. https://doi.org/10.1007/BF03340623
Kleiner C, Disterer G (2015) Ensuring mobile device security and compliance at the workplace. Procedia Comput Sci 64:274–281. https://doi.org/10.1016/j.procs.2015.08.490
Klipper S (2020) Weird sociotechnical systems. HMD 57:571–583. https://doi.org/10.1365/s40702-020-00606-x
Kraft R, Stöwer M (2017) IT-Risikomanagement im Produktionsumfeld – Herausforderungen und Lösungsansätze. HMD 54:84–96. https://doi.org/10.1365/s40702-016-0282-1
Kuhnert F, Stürmer C, Koster A (2018) Five trends transforming the automotive industry. PricewaterhouseCoopers,
Mayring P (2014) Qualitative content analysis: theoretical foundation, basic procedures and software solution. Universität Klagenfurt, Klagenfurt
Mohr D, Kaas H-W, Gao P, Wee D, Möller T (2016) utomotive revolution—perspective towards 2030: how the convergence of disruptive technology-driven trends could transform the auto industry, advanced industries. McKinsey,
Moody GD, Siponen M, Pahnila S (2018) Toward a unified model of information security compliance. MISQ 42(1):285–311. https://doi.org/10.25300/MISQ/2018/13853
Padyab AM, Päivärinta T, Harnesk D (2014) Genre-based approach to assessing information and knowledge security risks. Int J Knowl Manag 10:13–27. https://doi.org/10.4018/ijkm.2014040102
Potter A, Graham S (2019) Supplier involvement in eco-innovation: the co-development of electric, hybrid and fuel cell technologies within the Japanese automotive industry. J Clean Prod 210:1216–1228. https://doi.org/10.1016/j.jclepro.2018.10.336
Project Management Institute (2013) A guide to the project management body of knowledge, 5. Aufl.
Rauch A, van Doorn R, Hulsink W (2014) A qualitative approach to evidence-based entrepreneurship: theoretical considerations and an example involving business clusters. Entrep Theory Pract 38:333–368. https://doi.org/10.1111/etap.12093
Rechberg I, Syed J (2014) Knowledge management practices and the focus on the individual. Int J Knowl Manag 10:26–42. https://doi.org/10.4018/ijkm.2014010102
Reinheimer S, Weber K (2020) Faktor Mensch Teil 1 – vor-Corona-Phase. HMD 57:369–371. https://doi.org/10.1365/s40702-020-00619-6
Santos IM, Ali N (2012) Exploring the uses of mobile phones to support informal learning. Educ Inf Technol 17:187–203. https://doi.org/10.1007/s10639-011-9151-2
Schwab K (2017) The fourth industrial revolution, 1. Aufl. Crown Business, New York
Sowa A (2008) IT-Sicherheit durch Zugriffs- und Zugangskontrollen. HMD 45:78–88. https://doi.org/10.1007/BF03341252
Taylor A (2013) Information security management principles, 2. Aufl. BCS, the Chartered Institute for IT, Swindon
Teece DJ (2007) Explicating dynamic capabilities: the nature and microfoundations of enterprise performance. Strateg Manag J 28:1319–1350. https://doi.org/10.1002/smj.640
Tilson D, Lyytinen K, Sorensen C (2010) Desperately seeking the infrastructure in IS research: conceptualization of "digital convergence" as co-evolution of social and technical infrastructures. IEEE, S 1–10 https://doi.org/10.1109/HICSS.2010.141
Tremmel M (2021) Kundendaten von VW und Audi in Hackerforum angeboten. https://www.golem.de/news/nach-datenleck-kundendaten-von-vw-und-audi-in-hackerforum-angeboten-2106-157435.html. Zugegriffen: 21 Okt 2021
Vargo SL, Lusch RF (2004) Evolving to a new dominant logic for marketing. J Mark 68:1–17. https://doi.org/10.1509/jmkg.68.1.1.24036
Väyrynen K, Hekkala R, Liias T (2013) Knowledge protection challenges of social media encountered by organizations. J Organ Comput Electron Commer 23:34–55. https://doi.org/10.1080/10919392.2013.748607
Watson S, Hewett K (2006) A multi-theoretical model of knowledge transfer in organizations: determinants of knowledge contribution and knowledge reuse. J Manag Stud 43:141–173. https://doi.org/10.1111/j.1467-6486.2006.00586.x

Weber K (2020) Rezension „security awareness“. HMD 57:631–633. https://doi.org/10.1365/s40702-020-00617-8

Whitman M, Mattord H (2015) Ongoing threats to information protection. ACM Press, , S 1–2 https://doi.org/10.1145/2885990.2885994

Xu LD, Wang C, Bi Z, Yu J (2012) AutoAssem: an automated assembly planning system for complex products. IEEE Trans Ind Inform 8:669–678. https://doi.org/10.1109/TII.2012.2188901

Yi J (2009) A measure of knowledge sharing behavior: scale development and validation. Knowl Manag Res Pract 7(1):65–81. https://doi.org/10.1057/kmrp.2008.36

Yin RK (2018) Case Study Research and Applications: Design and Methods. Sage Publications Ltd. 6. ISBN 978-1-5063-3616-9