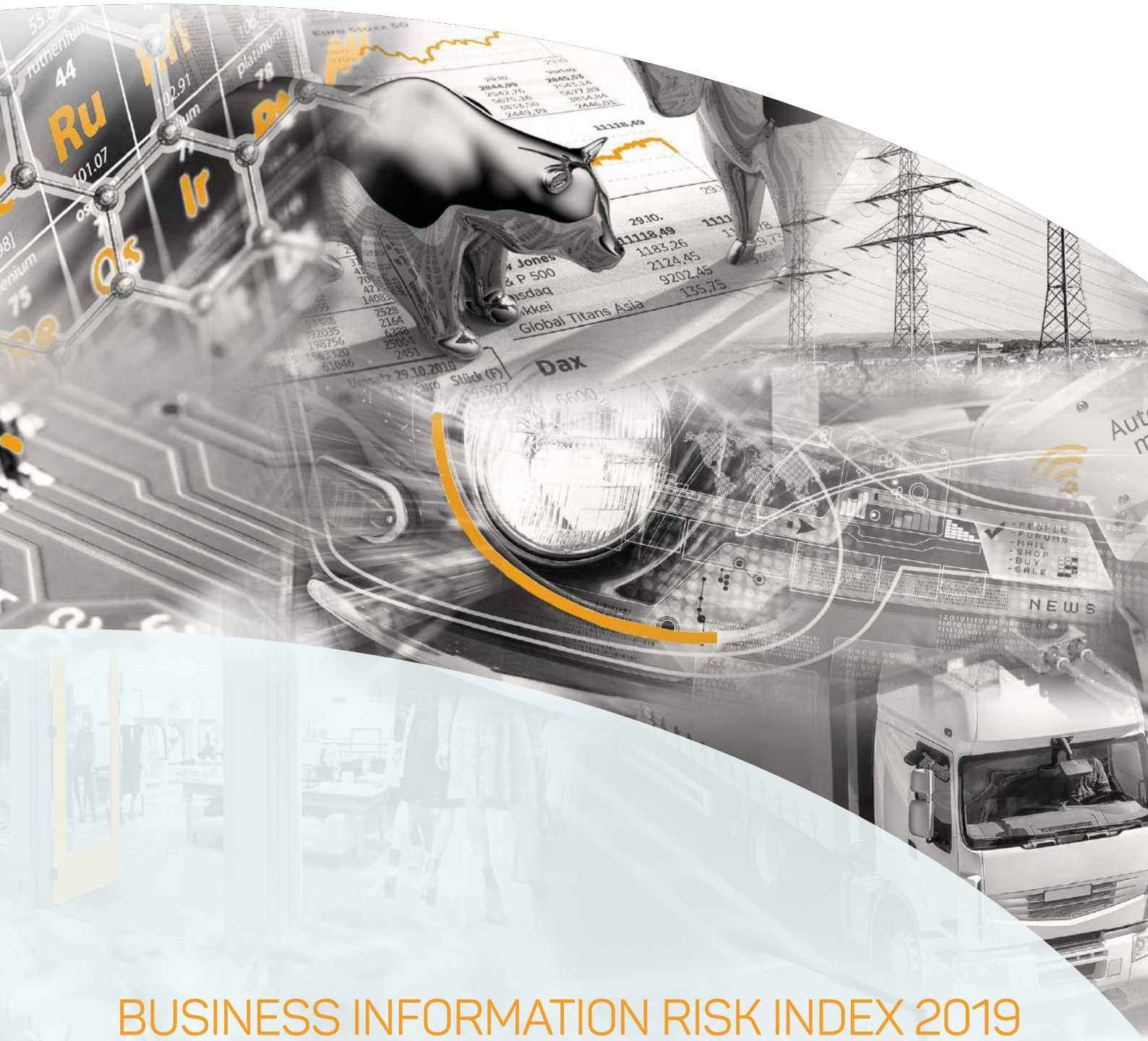
CISO ALLIANCE

QUALIFIZIEREN VERNETZEN FÖRDERN



BUSINESS INFORMATION RISK INDEX 2019

Wie vertrauen Business Manager ihrer Informationssicherheit?

Inhalt

VORBEMERKUNGEN
GEWALTIGE BRANCHENUNTERSCHIEDE

Selbst in den Tagesmedien sind die Informationssicherheit und Cyber-Gefahren durch die private Digitalisierung der Menschen zu einem gängigen Thema geworden, aber ist daraus der Schluss zu ziehen: Hoher Bekanntheitsgrad gleich hohes Sicherheitsbewusstsein?

Vielfältige Untersuchungen kommen zu gegenteiligen Erkenntnissen, insbesondere wenn es um die Informationssicherheit in der Wirtschaft geht. Wie sieht dort der aktuelle Status aus und wie unterscheiden sich möglicherweise die einzelnen Wirtschaftssektoren?

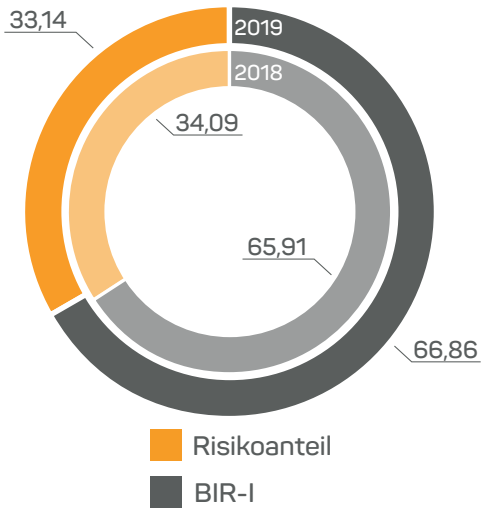
Um substanzielle Antworten darauf zu erlangen, hatte die CARMAO GmbH 2017 den Business Information Risk-Index (BIR-I) entwickelt, er wird inzwischen von der CISO Alliance weitergeführt. Die jährliche Untersuchung basiert für die Gesamtbetrachtung auf 10 Bewertungskriterien, die in einer Skala von 1 bis 10 bewertet werden und deren addierte Einzelwerte das Gesamtniveau und damit den Index-Wert ergeben. Als kritische Bereiche wurden Einzelbewertungen von unter 7,5 und Gesamtergebnisse von unter 75 Punkten bewertet.

Insgesamt wurden für die aktuelle Untersuchung 2.026 Business Manager aus Unternehmen mit einem Jahresumsatz von über 10 Mio. Euro in den zehn wichtigsten Branchen befragt. Somit wurde für jedes dieser Marktsegmente ein eigener Business Information Risk-Index ermittelt.

BRANCHENÜBERGREIFENDE BETRACHTUNG
BUSINESS INFORMATION RISK-INDEX STAGNIERT AUF NIEDRIGEM NIVEAU

Mit der Digitalisierung wächst die Angriffsfläche für Cyber-Bedrohungen aus dem Cyber-Raum, zu diesem klaren Ergebnis kommt eine diesjährige Studie des Bundesamtes für Informationssicherheit (BSI). Danach erwarten fast neun von zehn Institutionen von der Digitalisierung eine Verschärfung der Bedrohungslage, also dass mit der Digitalisierung zusätzliche Cyber-Risiken einhergehen und dass neben den sichtbaren Chancen auch die unsichtbaren Gefahren wachsen. Lediglich eine Minderheit von 8 Prozent ist optimistisch und glaubt nicht an zusätzliche Gefährdungen. Auch weitere Zahlen bestätigen die Problematik eindeutig: Im letzten Jahr waren 800 Millionen Schadprogramme im Umlauf, täglich kommen 390.000 neue Varianten hinzu.

Business Information Risk Index (BIR-I)
Alle Branchen



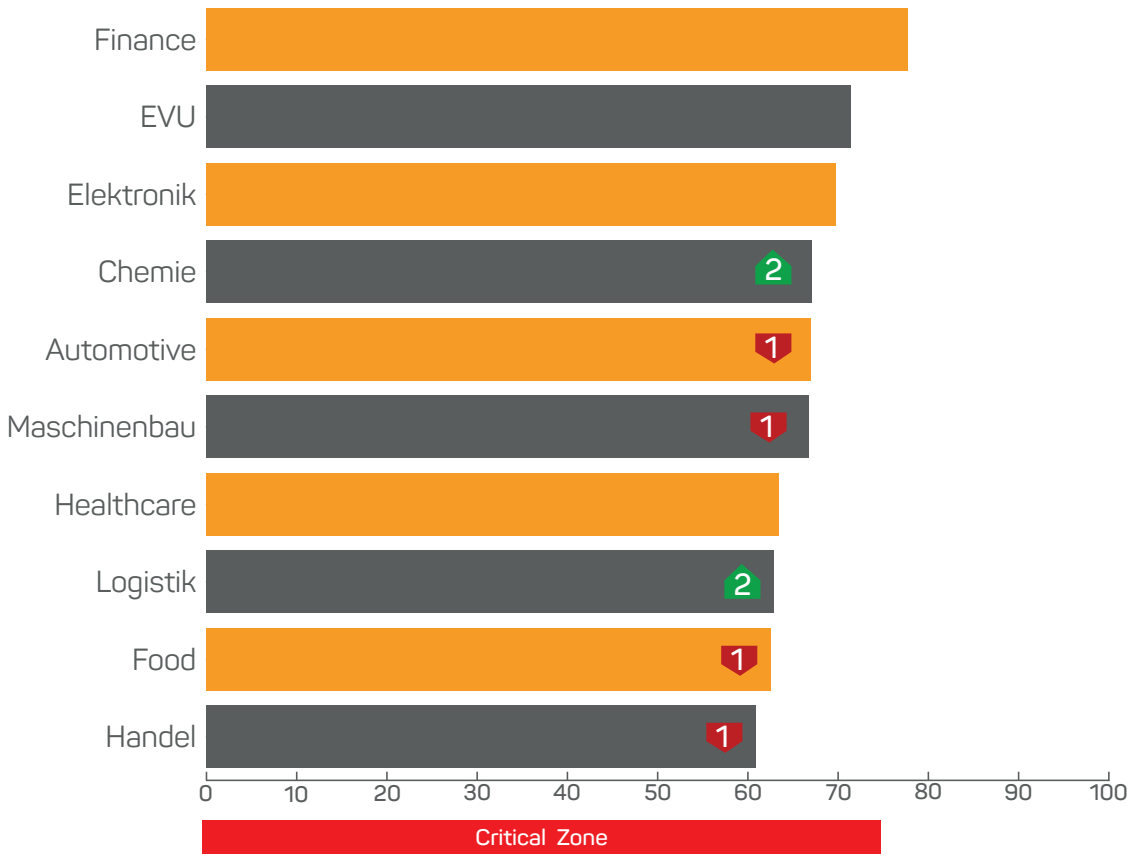
Die Situation: Je stärker der Digitalisierungsgrad und die Komplexität der Vernetzung von Systemen zunehmen, desto mehr gelangen sie wegen steigender Risiken auch in den Fokus der Informationssicherheit. Und auf diese Anforderungen scheinen die Unternehmen aktuell aus der Perspektive der Business Manager noch nicht ausreichend vorbereitet zu sein. So zumindest lassen sich die Ergebnisse der Befragung interpretieren, die branchenübergreifend einen Business Information Risk-Index von lediglich 66,86 erreicht. Er liegt damit deutlich unter dem Maximalwert von 100 und befindet sich deutlich in einem kritischen Bereich. Zudem hat er sich gegenüber 2017 lediglich um 3,62 Punkte verbessert.

Zu diesem Gesamtergebnis hat aus der Branchenbetrachtung heraus wesentlich beigetragen, dass für verschiedene Marktsegmente wie etwa die Lebensmittelindustrie, den Handel und auch die Logistikwirtschaft eine deutlich unterdurchschnittliche Situation in der Informationssicherheit ermittelt wurde.

Allerdings weist auch der Finanzsektor als die Branche mit dem höchsten Niveau an Informationssicherheit auch nur einen Index-Wert von 77,64 auf – nur knapp über die Critical Zone von 75.

Regelfall nur zurückhaltend in Sachen Informationssicherheit positioniert und sie auch in der Kommunikation zwischen den Führungskräften der zweiten Ebene nur zurückhaltend thematisiert wird.

Business Information Risk Level
Alle Branchen



In der Detailbetrachtung fällt auf, dass zwar das Sicherheitsniveau - im Vergleich zu anderen Aspekten - relativ hoch bewertet wird (7,24 von 10), aber das empfundene Risikobewusstsein im Unternehmen mit einem Wert von 7,02 deutlich niedriger ist. Beide Werte haben sich gegenüber 2017 sogar leicht verschlechtert. Zu den bemerkenswerten Auffälligkeiten gehört gleichermaßen, dass sich offensichtlich die Unternehmensführung im

Weitere kritische Erkenntnisse zeigen, dass die Business-Abteilungen in den letzten 12 Monaten im Regelfall nicht frei von Sicherheitsvorfällen geblieben sind und offenbar nur sporadisch Sicherheitsüberprüfungen stattfinden. Und bemerkenswert ist außerdem: Die Mitarbeiter werden in die Strategien zur Informationssicherheit meist nur sehr begrenzt einbezogen und über Awareness-Maßnahmen entsprechend fortgebildet und sensibilisiert.

AUTOMOTIVE
STOTTERNDER SICHERHEITSMOTOR

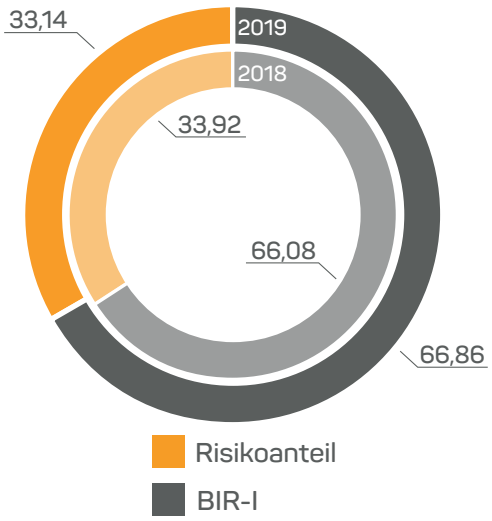
Abseits der Diskussion zur Dieselaffäre klingen die Perspektiven des technologischen Fortschritts des Autos durchaus spannend. Schließlich werden sie demnächst in einer hoch digitalisierten Weise selbstfahrend, elektrifiziert und vernetzt sein. Doch was äußerst innovativ klingt, bleibt trotzdem vorerst noch eine Vision von morgen mit sehr unbestimmtem Realisierungsdatum, denn die Stichworte autonomes Fahren, Elektromobilität oder Connected Cars skizzieren zwar die zukünftig neue Dimension des Produkts Auto und öffnen die Tür zu neuen Geschäftsmodellen. Vor allem aber gehen mit dieser Digitalisierung der Mobilität gleichzeitig auch neue Sicherheitsfragen von erheblicher Bedeutung einher.

Diese produktbezogenen Sicherheitsaspekte dürfen aber nicht den Blick davor verstellen, welchen Schutz die Automotive-Unternehmen selbst in ihrer betrieblichen und produktionsbezogenen Organisation gegen die Security-Risiken aufgebaut haben. Denn derzeit wird lediglich ein Business Information Risk-Index von 66,86 Punkten erreicht, gegen über dem Vorjahr eine kaum nennenswerte Steigerung um 0,78 Punkte.

Damit bleiben weiterhin die Anforderungen in den analysierten Leistungsaspekten der Informationssicherheit nicht einmal zu zwei Drittel erfüllt, wodurch sich diese Unternehmen durchschnittlich in der Critical Zone befinden.

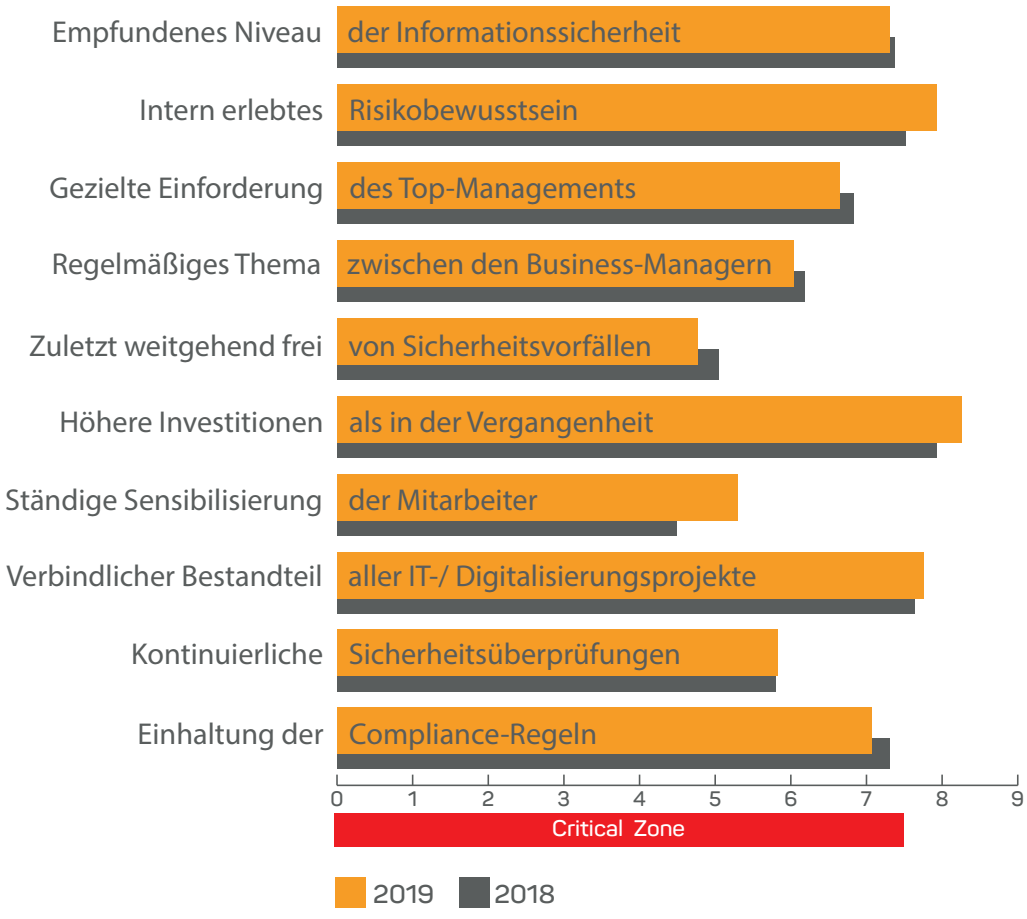
So verzeichnen sie im Vergleich zu den anderen untersuchten Branchen in überdurchschnittlicher Weise und seit 2017 kontinuierlich gestiegen sicherheitskritische Vorfälle wie digitale Wirtschaftsspionage, Sabotage oder Datendiebstahl. So beurteilen die befragten Business-Manager das

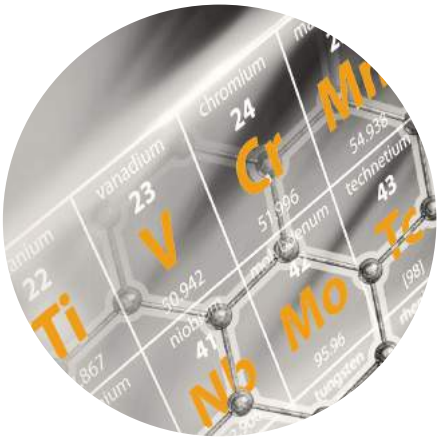
Business Information Risk Index (BIR-I)
Automotive



Niveau der empfundenen Informationssicherheit sogar niedriger als vor einem Jahr. Immerhin zeigen sich die Automotive-Firmen etwas weniger zurückhaltend bei der Sensibilisierung der Mitarbeiter für die Cyber-Gefahren. Vor allem aber wird stärker in die Unternehmens-Resilienz investiert – ein Anstieg von 7,92 auf 8,26 Punkte. Mit diesem Wert ist der Automotive-Sektor Investitionsspitzenreiter aller untersuchten Branchen.

Business Information Risk Level
Automotive



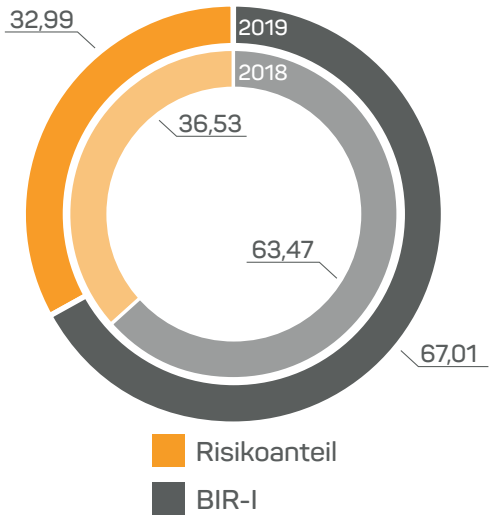


CHEMIE/PHARMA
ZWEITHÖCHSTES INVESTITIONS-ENGAGEMENT IM BRANCHENVERGLEICH

Drei Viertel der Chemie- und Pharmaunternehmen sind nach letztjährigen Erkenntnissen des Digitalverbandes Bitkom Opfer von Sabotage, Datendiebstahl oder Wirtschaftsspionage geworden. Und so langsam werden die notwendigen Konsequenzen vorgenommen, wie der aktuelle Business Information-Risk Index (BIR-I) für die chemisch-pharmazeutische Industrie zeigt. Mit 67,01 und einem Plus von 3,54 Punkten liegt er deutlich über dem des letzten Jahres, was im Ranking des Branchenvergleichs auch eine Verbesserung vom sechsten auf den vierten Platz bedeutet. Allerdings stellt dies keine Entwarnung da, weil unverändert gegenüber dem Maximalwert von 100 eine erhebliche Diskrepanz besteht.

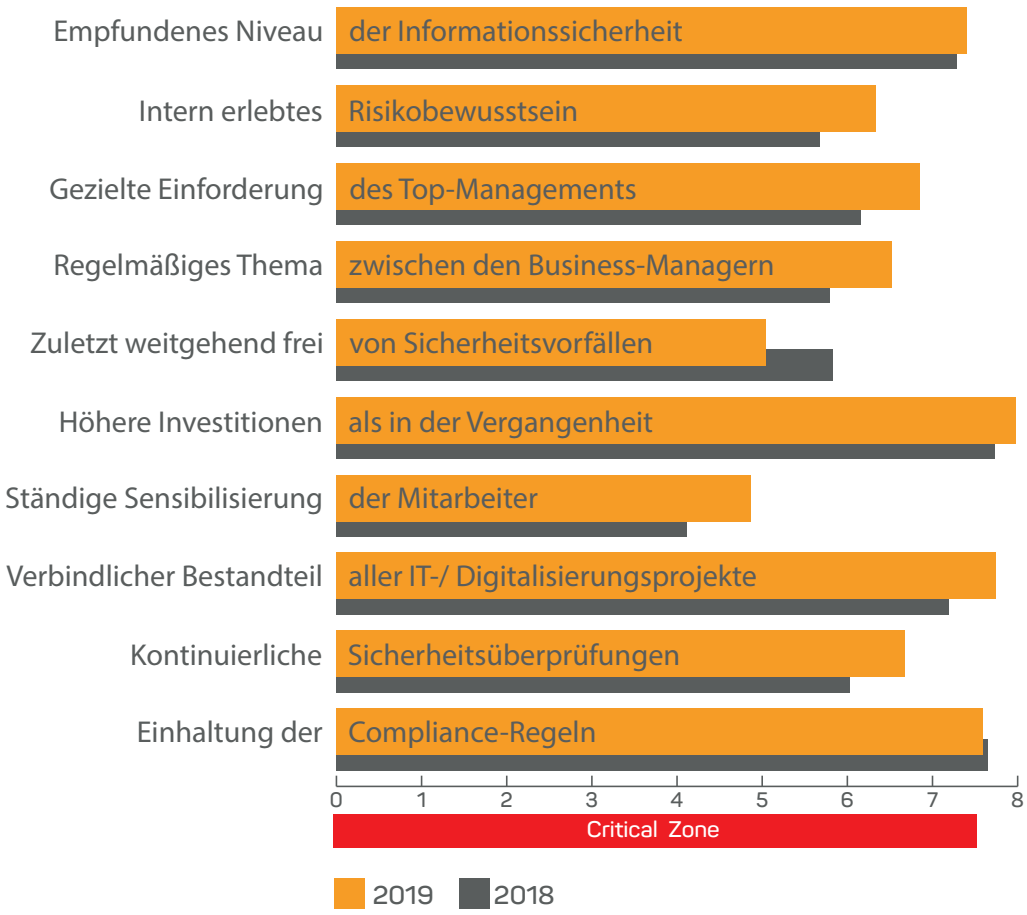
Auffällig ist auch für dieses Branchensegment, dass der empfundene Grad an Informationssicherheit gegenüber dem letzten Jahr gestiegen ist. Gleiches gilt für das Niveau des im Unternehmen vorhandenen Risikobewusstseins. Zudem haben die Sicherheitsüberprüfungen deutlich zugenommen und ist die Informationssicherheit häufiger ein Thema zwischen den Business-Managern auf den verschiedenen Hierarchieebenen.

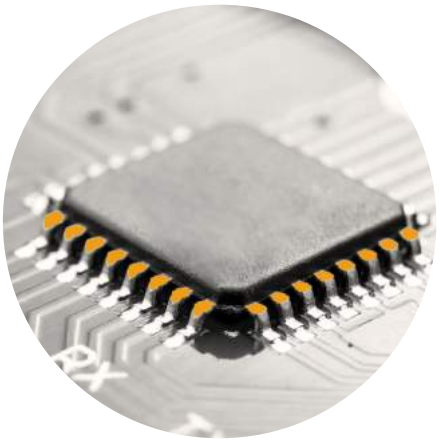
Business Information Risk Index (BIR-I)
Chemie/Pharma



Auch die Geschäftsleitung bringt sich mehr ein, indem sie das Security-Thema stärker intern positioniert hat. Dies drückt sich auch darin aus, dass von ihr zuletzt mehr Finanzmittel für Sicherheitsinvestitionen bewilligt wurden: Das Investitionsengagement weist im Branchenvergleich nach dem Automotive-Sektor den zweithöchsten Wert auf. Allerdings: Auch bei den Sicherheitsvorfällen belegt die chemisch-pharmazeutische Industrie den zweithöchsten Wert.

Business Information Risk Level
Chemie/Pharma



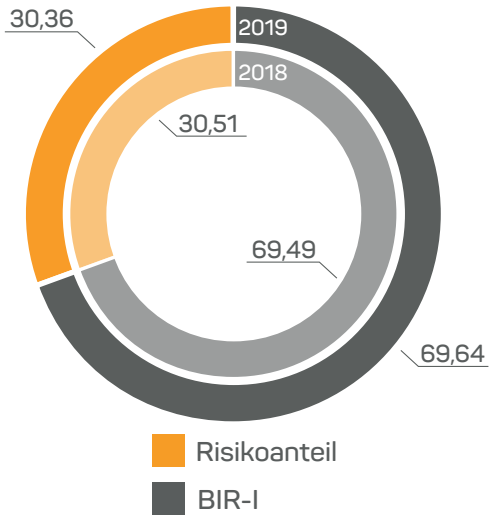


ELEKTRONIK
STAGNATION IN DER SECURITY-ENTWICKLUNG

Der Elektroniksektor versteht sich als Leitbranche der Digitalisierung, weil überall Elektronik mit im Boot ist, wo Produkte eine digitale Ausrichtung bekommen. Und dies gilt für IoT, Smart Home, die Mikroelektronik im Sinne von Industrie 4.0 und den selbstfahrenden Autos bei alle zukunftsträchtigen Technologien oder dem gesamten Entertainment-Bereich der Fall. Sie alle streben nach Vernetzung, was die Gefahrenpotenziale immer vielfältiger und gravierender macht.

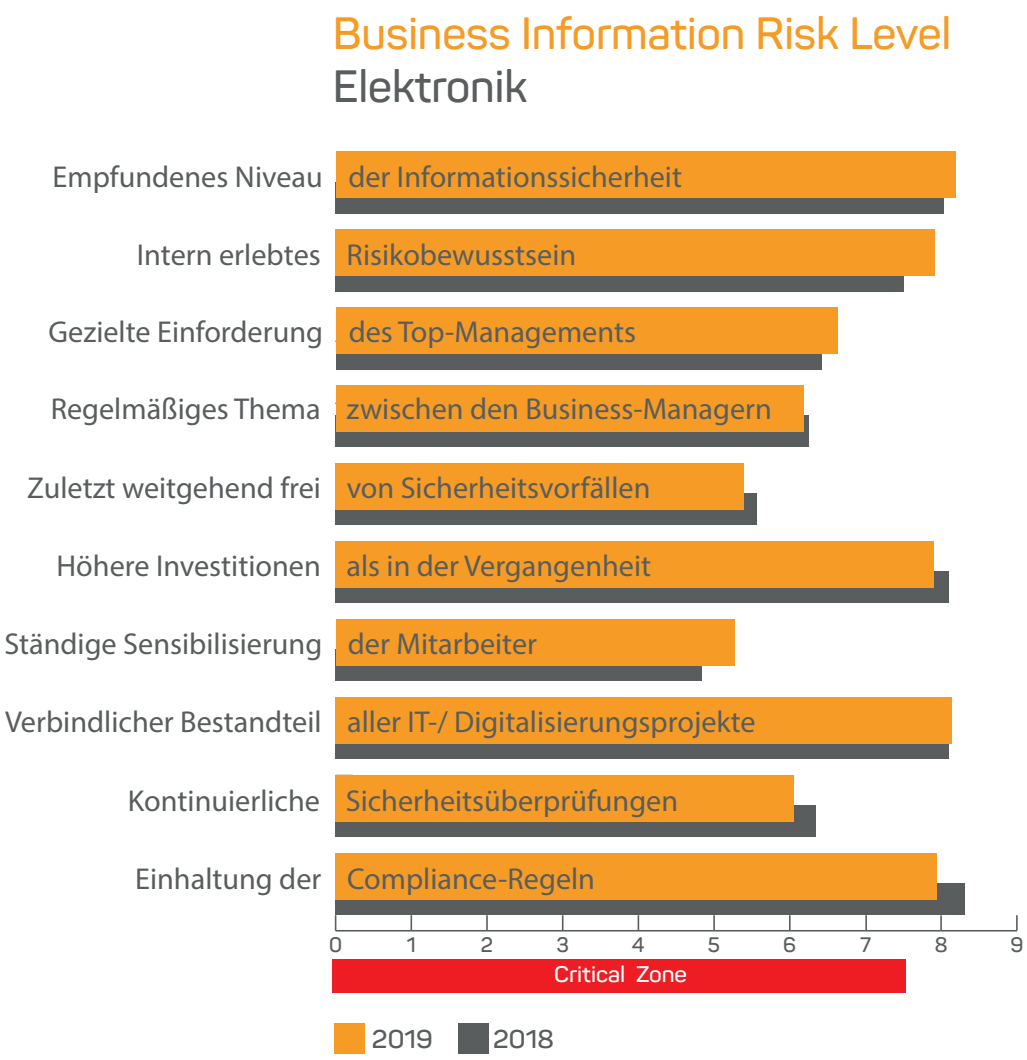
Demzufolge müssten die Elektronikhersteller ein hohes Sicherheitsengagement nicht nur bei der Fertigung vernetzungsfähiger Produkte, sondern – auch als Ausdruck von Sensibilität für das Thema – auch in ihrer Unternehmensorganisation aufweisen. Doch zumindest Letzteres ist nicht der Fall, weil die Informationssicherheit als Strategiethema in diesen Unternehmen noch längst nicht ausreichend ausgeprägt ist. Dies drückt der aktuelle Business Information Risk-Index (BIR-I) von 69,64 aus. Er stagniert gegenüber dem Vorjahr, nachdem er von 2017 auf 2018 noch um 4,18 Punkte gestiegen war. Zwar belegt der Elektroniksektor im Branchenranking weiterhin den dritten Platz, befindet er sich jedoch weiterhin deutlich in der unterhalb von 75 beginnenden Critical Zone.

Business Information Risk Index (BIR-I)
Elektronik



Dabei ist das empfundene Niveau der Informationssicherheit überdurchschnittlich hoch und weist mit einem Teilindex von 8,19 den höchsten Wert aller Branchen auf. Auch das Risikobewusstsein im Unternehmen ist gegenüber 2018 sogar deutlich gestiegen. Dafür haben sich andere Bewertungskriterien etwas verschlechtert, dies gilt etwa für die registrierten Sicherheitsvorfällen. Zudem stagniert der Teilindex in Bezug darauf, ob Sicherheitsaspekte grundsätzlich fester

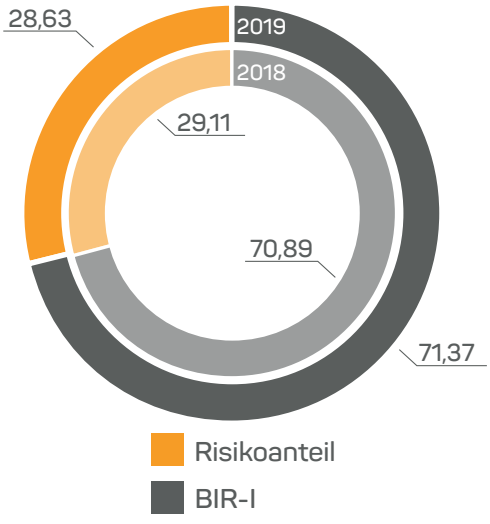
Bestandteil aller IT-/ Digitalisierungsprojekte sind. Ebenso sind die Investitionen in die Informationssicherheit gegenüber dem Vorjahr etwas zurückgegangen, auch wenn sie mit 7,91 oberhalb der Critical Zone und unverändert deutlich über dem Durchschnitt aller untersuchten Branchen liegen.



ENERGIEVERSORGER
ZWEITER BRANCHENRANG TROTZ DEUTLICHER SCHWÄCHEN

Die Energieversorger unterliegen aus gutem Grund besonderen regulativen Verpflichtungen wie etwa durch das IT-Sicherheitsgesetz, das Gesetz zur Umsetzung der Richtlinie zur Netzwerk- und Informationssicherheit (NIS) oder den IT-Sicherheitskatalog. Doch auch wenn die meisten Hacker-, Denial-of-Service-, Malware- oder Ransomware-Angriffe bisher keine direkten physischen Schäden zur Folge hatten, weil sie sich bisher überwiegend aif das Ausspionieren von Daten fokussierten, ist es möglicherweise nur noch eine Frage der Zeit, bis cyber-kriminelle Aktivitäten deutlich umfassendere Schäden erzeugen werden.

Business Information Risk Index (BIR-I)
Energieversorger

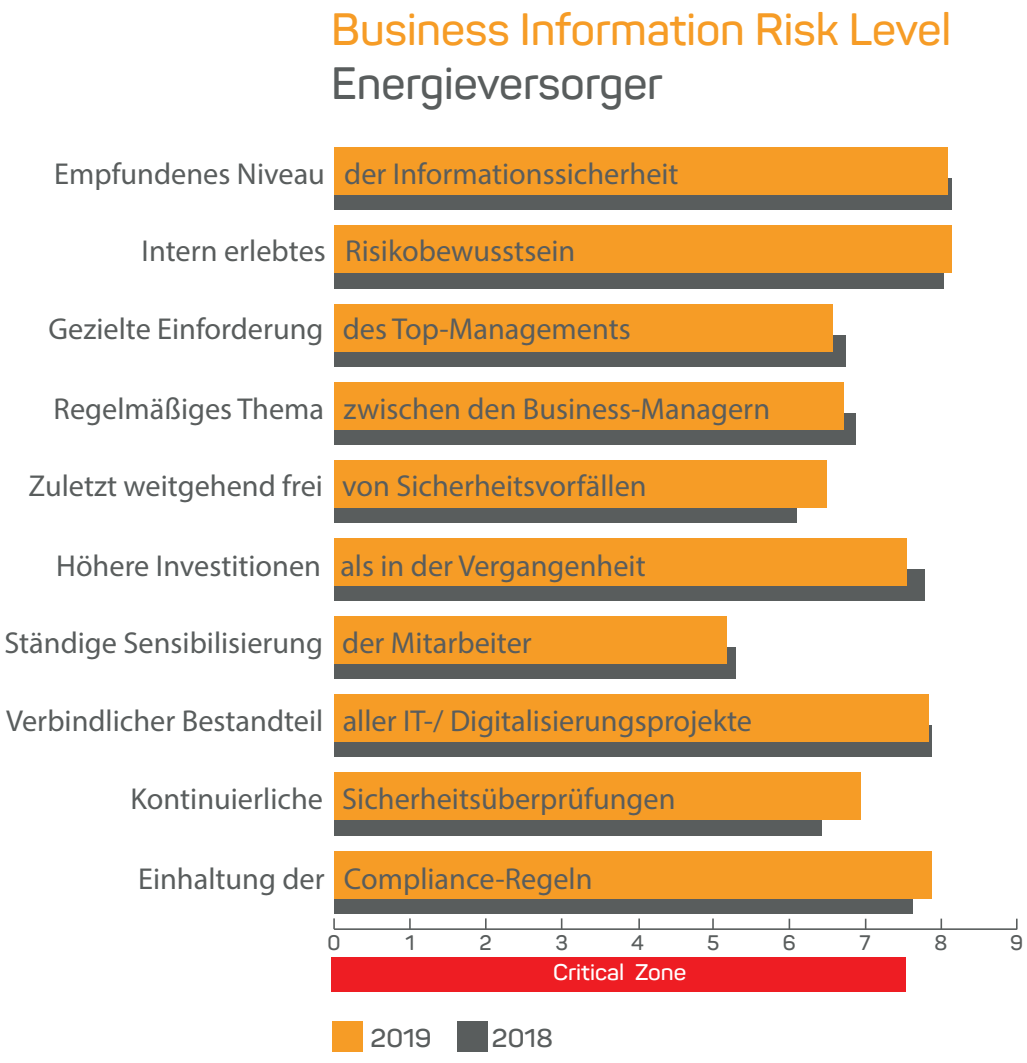


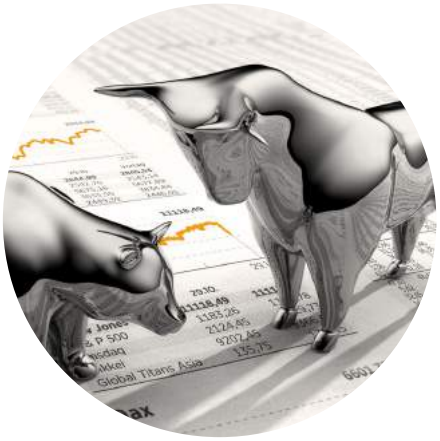
Auch deshalb, weil die Energieversorgung beispielsweise durch intelligente Stromnetze oder den Einbau von Smart Metern noch angreifbarer werden wird.

Trotzdem haben sich die Energieversorger in der Informationssicherheit trotz des regulativen Drucks im Branchendurchschnitt noch längst nicht auf ein Niveau gebracht, das als unkritisch bezeichnet werden könnte. Denn auch wenn der Business Information Risk-Index im Branchenvergleich wie in den Vorjahren den zweiten Rang erreicht und mit 71,37 Punkten leicht über dem Wert von 2018 liegt, bleibt er deutlich unterhalb der mit 75 Punkten definierten kritischen Grenze. Hintergrund ist, dass nur die Hälfte der zehn Teil-Indices die kritische Marke überschreiten, dazu gehören das empfundene Niveau der Informationssicherheit, das erlebte Risikobewusstsein und der Grad der Orientierung an den Compliance-Regeln.

Für alle anderen Aspekte werden in der Untersuchung hingegen weniger zufriedenstellende bis deutlich kritische Ergebnisse ermittelt – auch wenn sie allesamt über dem Branchendurchschnitt liegen und unterschiedliche Entwicklungsrichtungen aufweisen. So hat

sich die Situation bei den registrierten Schadensvorfällen in den letzten 12 Monaten auf einem allerdings deutlich unbefriedigenden Niveau etwas verbessert. IT-Sicherheit als strategisches Thema hat zudem und trotz der entsprechenden regulativen Einflüsse auf den Managementebenen etwas an Bedeutung verloren. Dagegen finden mehr Sicherheitsüberprüfungen statt und wird der Sensibilisierung der Mitarbeiter durch Awareness-Maßnahmen eine größere Relevanz beigemessen.



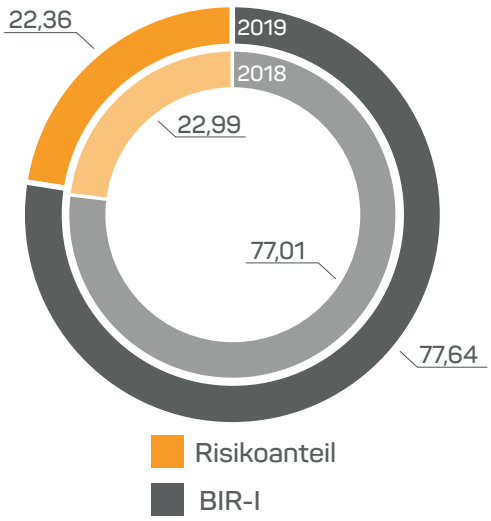


FINANCE
UNTERDURCHSCHNITTLICHE INVESTITIONSBEREITSCHAFT

IT-Infrastrukturen mit Legacy-Systemen, heterogenen Verhältnissen, komplizierten Schnittstellenarchitekturen und veralteten Programmiersprachen bedeuten eine Einladung für die Cyber-Kriminalität, weil sie durchgängig wirkungsvolle Abwehrstrategien schwer machen. Nicht ohne Grund warnt die Aufsichtsbehörde Bafin regelmäßig, dass die IT der Kreditinstitute dadurch anfällig für Angriffe von innen und außen ist. Die Blockchain-Technologien, inzwischen gerne als Allheilmittel genannt, können allein keine ausreichende Antwort auf diese sicherheitstechnischen Infrastrukturschwächen sein.

So ist möglicherweise zu verstehen, dass den Banken und Versicherungen das Vertrauen in die eigene Informationssicherheit verloren geht. Denn ihr selbst empfundenes Sicherheitsniveau zeigt im Business Information Risk-Index (BIR-I) für die Finanzwirtschaft für die letzten drei Jahre eine konstante Entwicklung nach unten. Lag er 2017 noch bei 8,44 und im letzten Jahr bei 8,16 Punkten, so hat er aktuell nur noch einen Wert von 7,93. Zudem hat sich die Situation bei den Sicherheitsvorfällen leicht verschlechtert, was wohl auch dazu beigetragen haben dürfte, dass die Ausprägung des Sicherheitsbewusstseins in den letzten 12 Monaten gestiegen ist.

Business Information Risk Index (BIR-I)
Finance



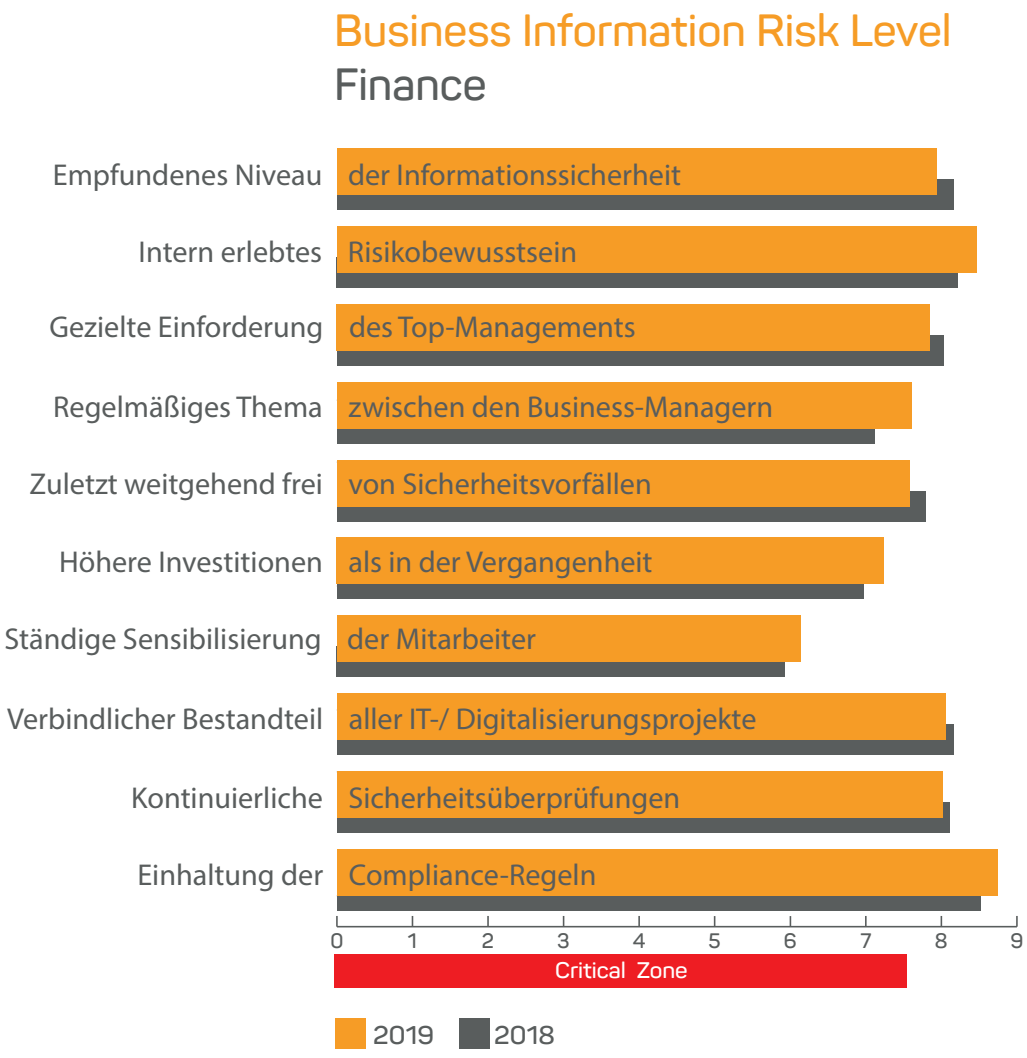
Dies sind jedoch nicht die einzigen Auffälligkeiten der Ergebnisse für die Finanzwirtschaft. Dazu gehört etwa auch, dass im Top-Management das Sicherheitsthema etwas an Bedeutung verloren hat, während es hierzu mehr Kommunikation zwischen den Managern der verschiedenen Hierarchieebenen gibt.

Bemerkenswert ist insgesamt, dass jedes zweite Ergebnis der zehn verschiedenen Parameter gegenüber dem Vorjahr eine nega-

tive Entwicklung zeigt. Dazu gehören auch die Werte für die Berücksichtigung von Sicherheitsaspekten als grundsätzlich fester Bestandteil aller IT-/ Digitalisierungsprojekte und für die Durchführung von Sicherheitstests.

Positiv lässt sich hingegen die etwas verstärkte Intensität in den Mitarbeiterschulungen vermerken, vor allem auch ist die Investitionsbereitschaft weiter gestiegen. Sie hat nach 2018 nochmals zugelegt. Andererseits:

Mit einem Einzelwert von 7,24 liegt das Investitionsengagement unverändert unterhalb der kritischen Grenze. Er ist damit unzureichend und liegt sogar unterhalb des Branchendurchschnitts, gleichzeitig nimmt der Finanzsektor beim Investitionsverhalten lediglich den sechsten Rang im Branchenvergleich ein.

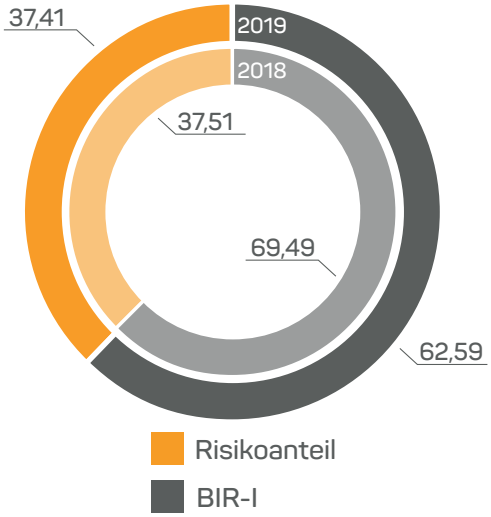


FOOD
WENIG LUST AUF IT-SICHERHEIT

Langsam beginnt die Digitalisierung auch in der Ernährungswirtschaft Fuß zu fassen, zumindest diskutiert die Branche unter dem Stichwort Lebensmittelindustrie 4.0 inzwischen verstärkt darüber. Dieser Ansatz steht für eine sich selbst organisierende Produktion, bei der Produktionsanlagen, logistische Systeme, Produkte und Menschen mit moderner Informations- und Kommunikationstechnologie digital miteinander vernetzt sind. Dies berührt zwangsläufig die Sicherheitsfrage, weil sie allen digitalen Initiativen innewohnt. Denn wo jetzt schon IP-gesteuerte Robotersysteme in den Produktions- und Verpackungsprozessen bestehen, bedarf es nicht erst zukünftig adäquater Sicherheitsverhältnisse, sie sind heute bereits zwingend erforderlich.

Aber davon ist bei den Food-Unternehmen auf breiter Front noch wenig zu sehen. Ihr Business Information Risk-Index (BIR-I) liegt aktuell lediglich bei 62,49, sogar etwas weniger als 2018: Nur ein weiterer Sektor verzeichnet einen Rückgang, weshalb die Lebensmittelindustrie im Branchenvergleich von achten auf den neunten und damit vorletzten Platz zurückfällt.

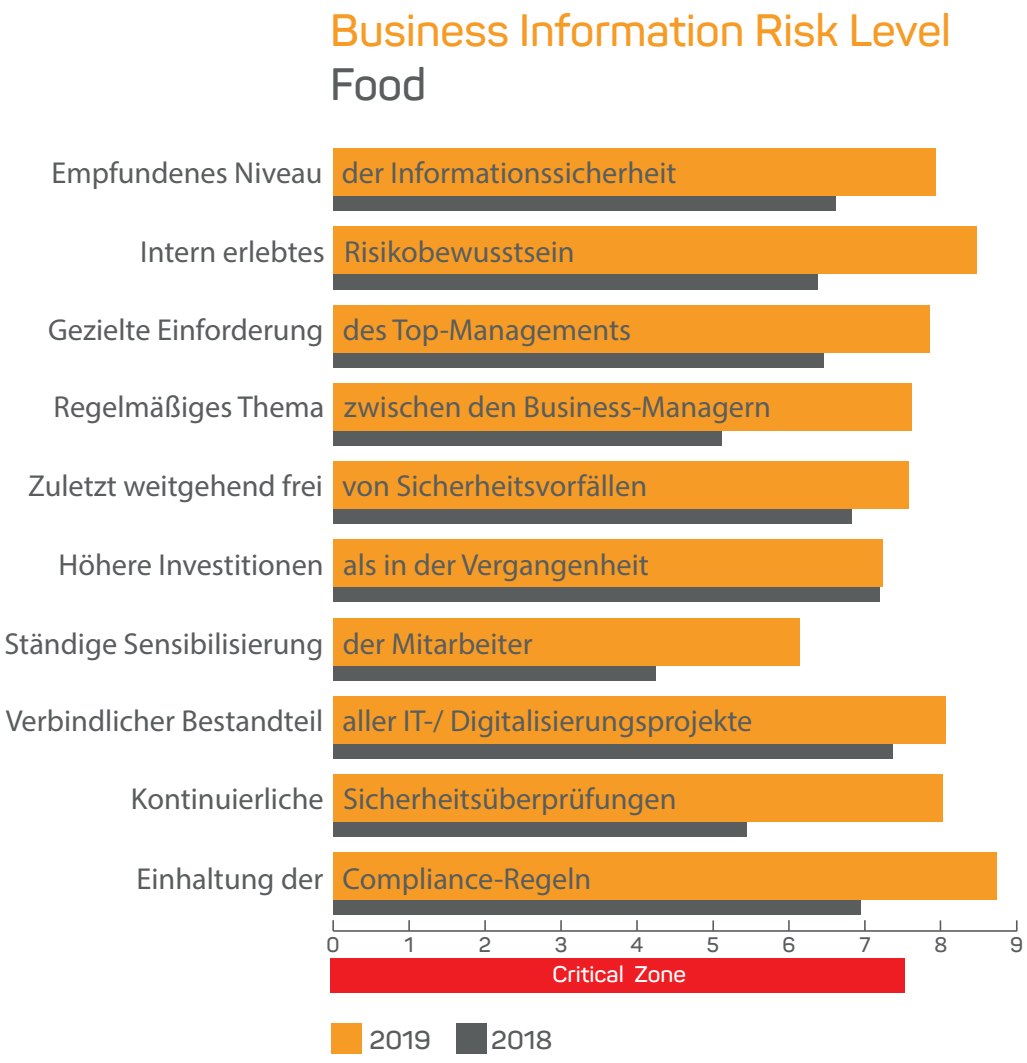
Business Information Risk Index (BIR-I)
Food



Dies resultiert nicht zuletzt daraus, dass das empfundene Sicherheitsniveau und interne Risikobewusstsein schlechtere Werte als im Vorjahr erreichen. Ebenso hat sich im Gesamtergebnis niedergeschlagen, dass es so deutlich wie in nur wenigen anderen Branchen an gezielten sicherheitsstrategischen Vorgaben des Top-Managements fehlt, die Informationssicherheit zu erhöhen. Auch zwischen den Business-Managern findet die Informationssicherheit als relevantes Thema kaum statt. Zu den sehr kritischen Aspekten gehört zudem, dass kaum regel-

mäßige Sicherheitsüberprüfungen in den Food-Unternehmen stattfinden.

Einen Lichtblick bietet auch das Investitionsverhalten in die Abwehr der wachsenden Cyber-Gefahren nicht. Zwar war dieser Wert 2018 gegenüber 2017 deutlich gestiegen, er ist mit einem Wert von 7,14 zwischenzeitlich aber wieder rückläufig und liegt damit deutlich unter dem Mittelwert aller untersuchten Branchen.



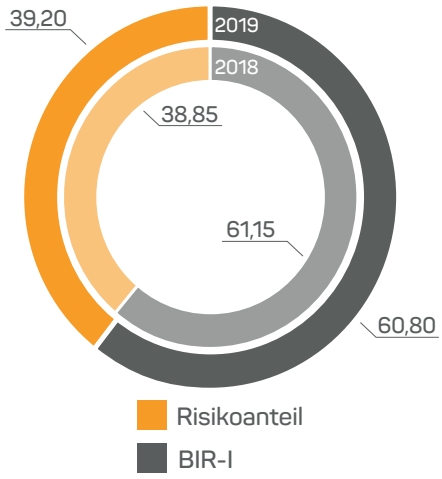
HANDEL
SCHLUSSLICHT IM BRANCHENVERGLEICH

Nicht nur das klassische Konsumergeschäft wird durch die Online-Alternativen Amazon & Co. kräftig aufgemischt, auch der Handel zwischen den Unternehmen läuft immer mehr elektronisch. Er macht bereits ein Viertel der B2B-Umsätze aus und hat 2018 ein Volumen von 320 Milliarden Euro erreicht. Allein aus dieser Digitalisierungsentwicklung im Retail-Business könnte abgeleitet werden, dass parallel dazu auch die Informationssicherheit in den Handelsunternehmen einen wachsenden Stellenwert erlangt hat.

Doch genau das Gegenteil ist der Fall, belegt durch den Business Information Risk-Index (BIR-I). Mit seinem aktuellen Wert von 60,80 liegt die Handelsbranche deutlich unterhalb des Branchendurchschnitts von 66,86 und um etwa ein Viertel unter dem des Finanzsektors. Damit rutschen die Handelsunternehmen im Branchenvergleich um einen Platz auf die letzte Position zurück.

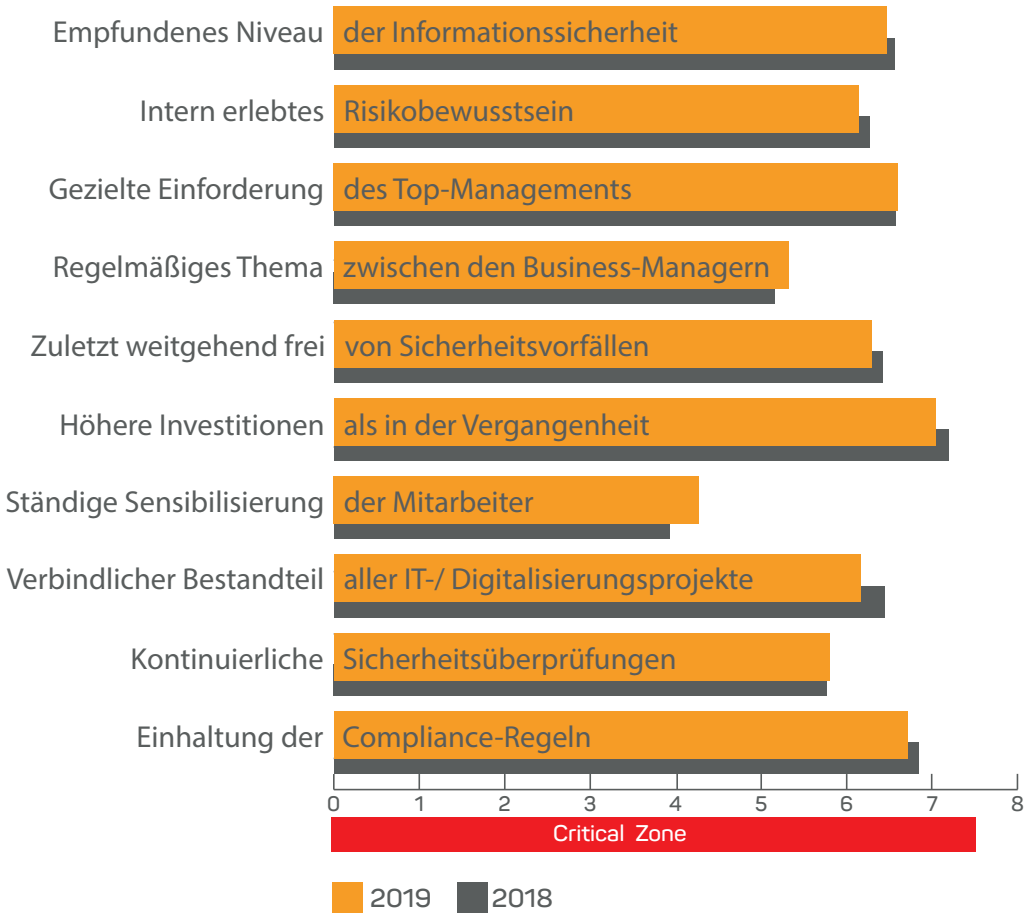
Zusätzlich bestehen gewisse Indikatoren, die eine zukünftig positivere Entwicklung derzeit fraglich machen. Dazu gehört, dass das von den befragten Business Managern wahrgenommene Sicherheitsniveau ebenso wie das empfundene Risikobewusstsein in den Unternehmen rückläufig ist. Weiterhin sind die Investitionsbemühungen gegenüber 2018 gesunken, während viele andere untersuchten Branchen einen Anstieg verzeichnen.

Business Information Risk Index (BIR-I)
Handel



Nicht zuletzt der Teilindex für die Sicherheitsvorfälle zeigt gegenüber dem Vorjahr einen schlechteren Wert, doch selbst die konkret erlebten Risiken scheinen bei den Unternehmen kein Umdenken in Richtung eines höheren Sicherheitsengagements zu erzeugen. Vor allem aber: Es lassen sich auch in allen anderen Ergebnissen der gesamten Bewertungskriterien keinerlei Hinweise erkennen, die darauf hindeuten.

Business Information Risk Level
Handel



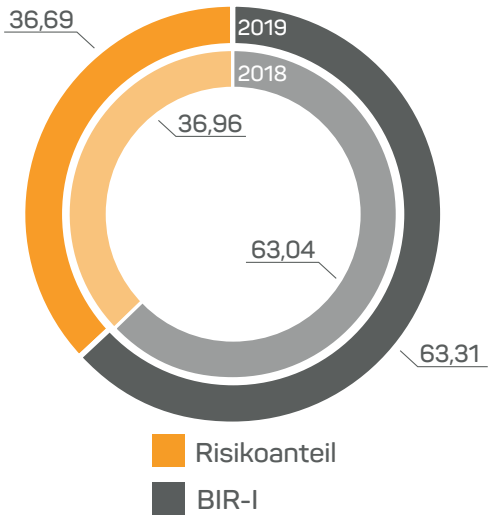
HEALTHCARE
DIE SCHWÄCHEN BEGINNEN OBEN

Gesundheitsdaten enthalten umfassende personenbezogene Informationen zu den individuellen Krankheitsgeschichten, detaillierte Diagnosen und Therapien, weshalb sie äußerst schützenswert sind und vor fremden Zugriffen abgesichert sein müssen. Auch den Schutz vor Manipulationen und missbräuchlichen Eingriffen in die medizinischen Prozesse gilt es zu gewährleisten, zumal mit eHealth die Digitalisierung auch die Gesundheitsversorgung erreicht hat. Sie bietet grundsätzlich ein vielfältiges Potenzial zur besseren Patientenversorgung und Kosteneinsparungen, macht andererseits aber auch den Bedarf an einer hohen Informationssicherheit notwendig.

Das IT-Sicherheitsgesetz, nach dem auch größere Krankenhäuser zu kritischen Infrastrukturen gezählt werden und sie demzufolge die Anforderungen der BSI-Kritis-Verordnung erfüllen müssen, geht in diese Richtung. Aber betroffen davon sind lediglich Krankenhäuser und Pflegeeinrichtung mit mehr als 30.000 vollstationären Behandlungsfällen, alle anderen können demzufolge ihre IT-Sicherheitsstrategien weniger ambitioniert gestalten.

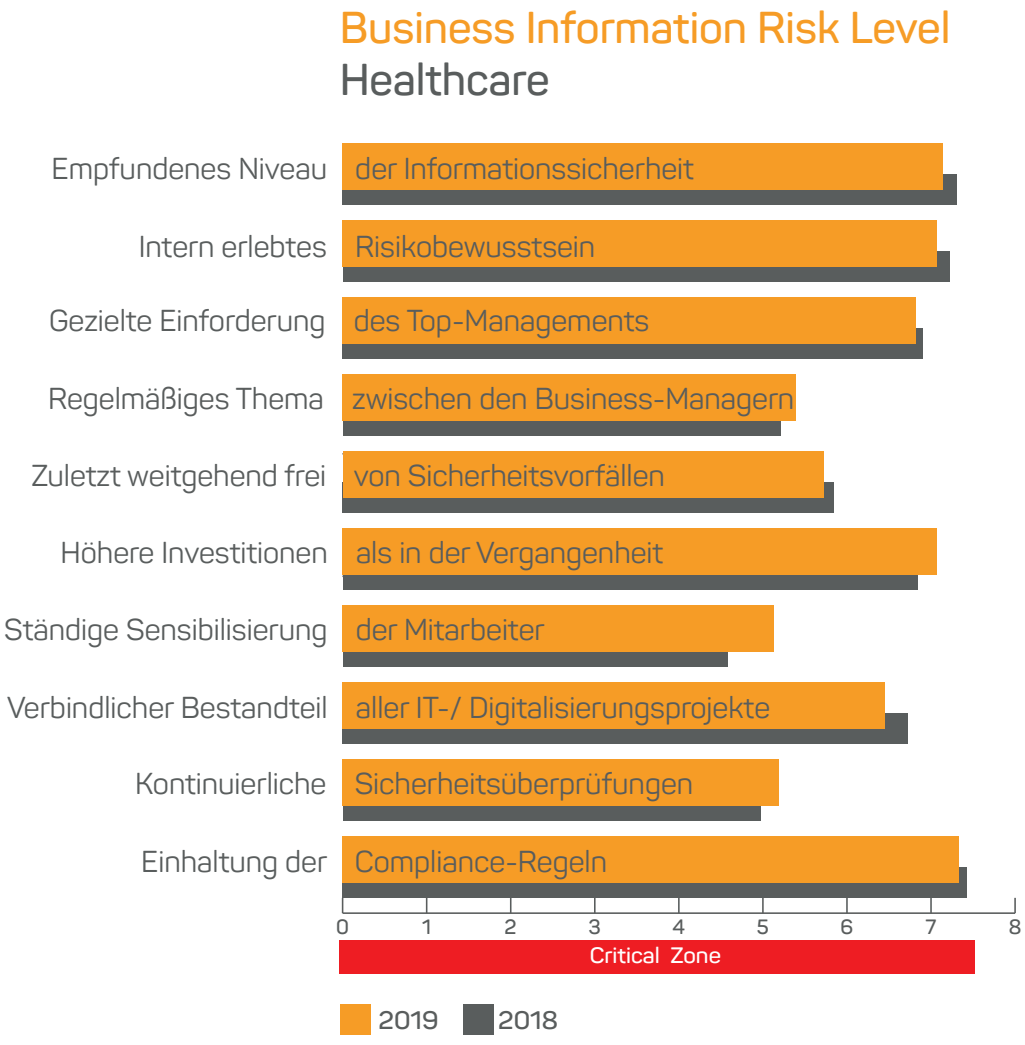
Dies bildet sich auch im Business Information Risk-Index (BIR-I) für den Healthcare-Sektor ab. Er liegt aktuell bei 63,31 Punkten und damit nur wenig verändert gegenüber dem

Business Information Risk Index (BIR-I)
Healthcare



letzten Jahr und gleichzeitig deutlich in der kritischen Zone. Dabei wird das empfundene Sicherheitsniveau und das interne Risikobewusstsein keineswegs kritisch eingeschätzt, es liegt allerdings auch nur auf der Ebene der branchenübergreifenden Mittelwerte.

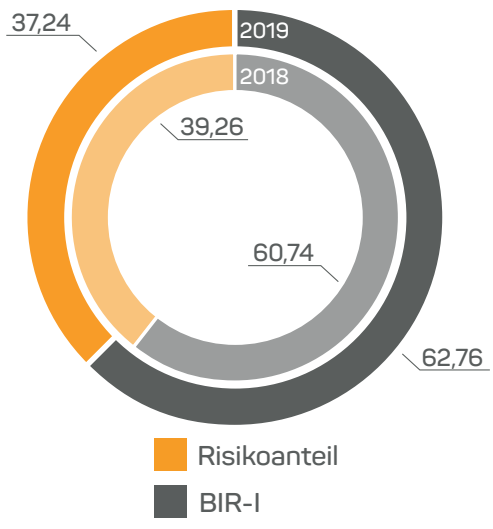
Allerdings wird deutlich zu wenig in die Informationssicherheit investiert, nur der Handel und der Logistiksektor weisen hier noch geringere Werte auf. Auf der Negativseite steht zudem, dass vergleichsweise wenig für die sicherheitsbezogene Mitarbeiterschulung getan wird und auch Sicherheitsüberprüfungen relativ selten stattfinden. Was insofern nicht wundert, weil sich die Geschäftsleitung und auch das Management darunter des Sicherheitsthemas zu wenig annehmen.



LOGISTIK
NUR VERBESSERUNGEN AUF GERINGEM NIVEAU

Elektronisch gestützte Prozesse setzen sich bei den Verladern, Spediteuren und Transportunternehmen immer mehr durch. Flotten werden vernetzt und digital im Auge behalten, immer mehr Logistiker setzen auf eine zentrale Steuerung des Warenversands. Und auch wenn sich immer mehr Branchenführer auf die digitalen Bedrohungssituationen versuchen einzustellen, ist gerade der logistische Mittelstand noch weit von ausreichenden Sicherheitsbedingungen entfernt und findet Security eine deutlich zu geringe Beachtung.

Business Information Risk Index (BIR-I)
Logistik

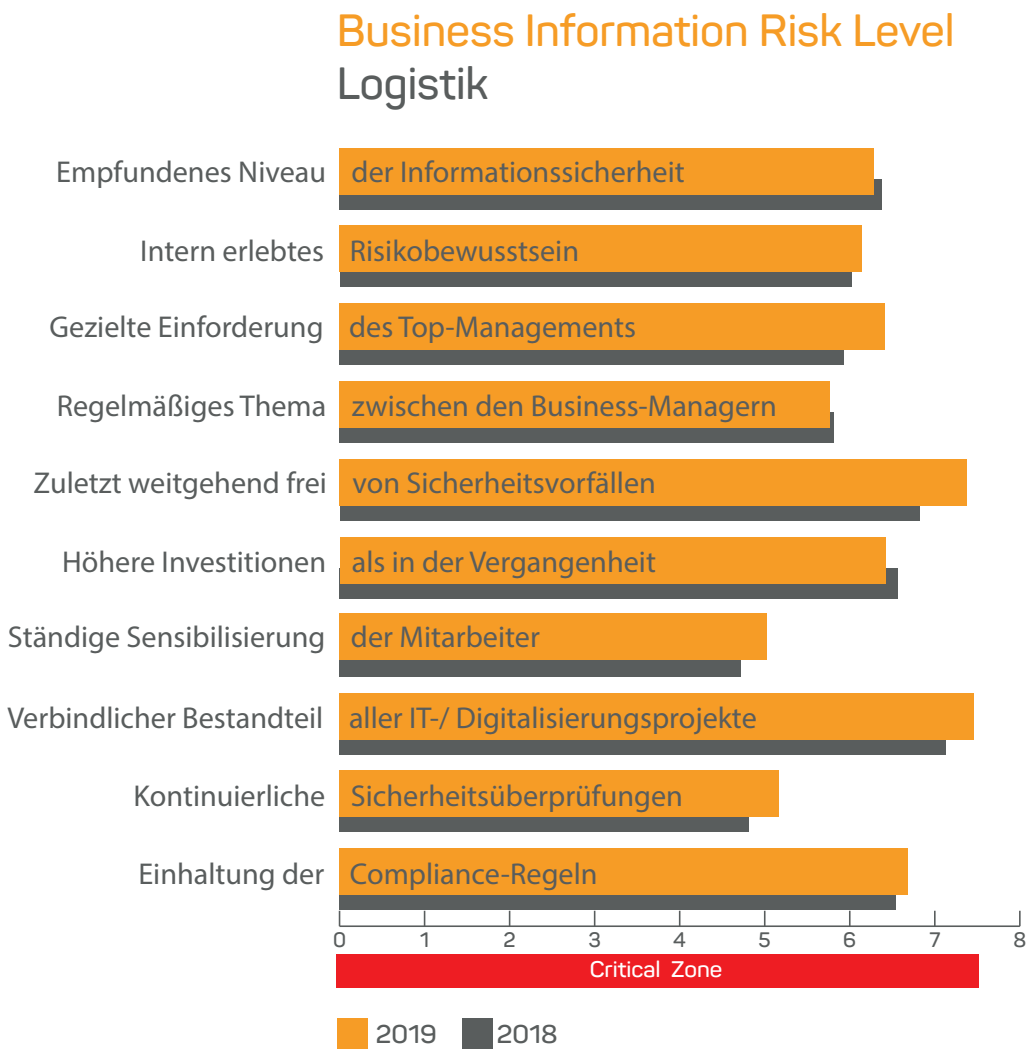


Dies gilt besonders für das aktuelle Niveau der Informationssicherheit aus Sicht der befragten Business Manager, das mit einem Teilindex von 6,29 Punkten von allen zehn untersuchten Branchen den geringsten Wert aufweist und sogar noch geringer ist als im letzten Jahr. Ein ebenso geringes Niveau verzeichnet das interne Risikobewusstsein. Dieses Meinungsbild resultiert möglicherweise auch daraus, dass im Vergleich mit allen anderen Branchen in den letzten 12 Monaten in unterdurchschnittlichem Umfang Sicherheitsvorfälle registriert wurden.

Andererseits dürfte zu den zentralen Ursachen auch gehören, dass eine unzureichende Kultur hinsichtlich der Informationssicherheit besteht. Dies drückt sich auch darin aus, dass sie von den Verantwortlichen auf allen Ebenen nur begrenzt thematisiert wird. Zudem finden in keiner Branche so selten Sicherheitsüberprüfungen statt wie in den Logistikbetrieben. Auch die Investitionsbereitschaft zeigt gegenüber den anderen Wirtschaftssektoren ein unterdurchschnittliches Ergebnis.

Dafür finden häufiger Sicherheitsüberprüfungen als in der Vergangenheit statt, werden

die Mitarbeiter stärker zu den Sicherheitsrisiken geschult und sind Sicherheitsaspekte verstärkt fester Bestandteil aller IT-/ Digitalisierungsprojekte. Dadurch ist der Business Information Risk-Index (BIR-I) gegenüber 2018 um etwa zwei Punkte auf 62,76 gestiegen, wodurch die Logistik vom letzten Platz des Branchenrankings im letzten Jahr auf die achte Position vorgerückt ist. Dies ändert aber nichts daran, dass sich ihr Sicherheitsniveau unverändert deutlich im kritischen Bereich befindet.



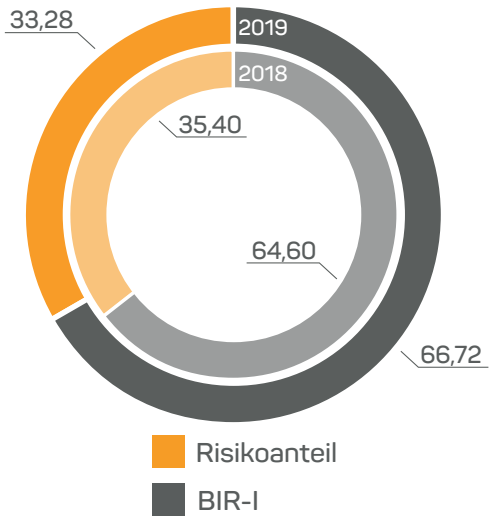
MASCHINENBAU
UNSICHER RICHTUNG INDUSTRIE 4.0

Die Digitalisierung ist auch in der Maschinenbauindustrie angekommen. Spätestens mit der Etablierung cyber-physischer Systeme und deren Vernetzung sowohl untereinander als auch mit internetbasierten Software-Services wird Industrie 4.0 in den Unternehmen des Maschinen- und Anlagenbaus einen durchgreifenden Wandel erzeugen. Deswegen muss aber keineswegs unbedingt eine übergreifende Vernetzung von Produktionsstrukturen entstehen, doch ganz gleich, welcher Komplexitätsgrad in der Vernetzung zukünftig die Maschinenbauindustrie prägen wird: Die Unternehmen sind darauf vielfach noch nicht vorbereitet, weil viele Systeme nicht den heutigen Sicherheitsanforderungen entsprechen und an den Shop-Floors häufig auch das Know-how in Sachen Cyber-Security fehlt.

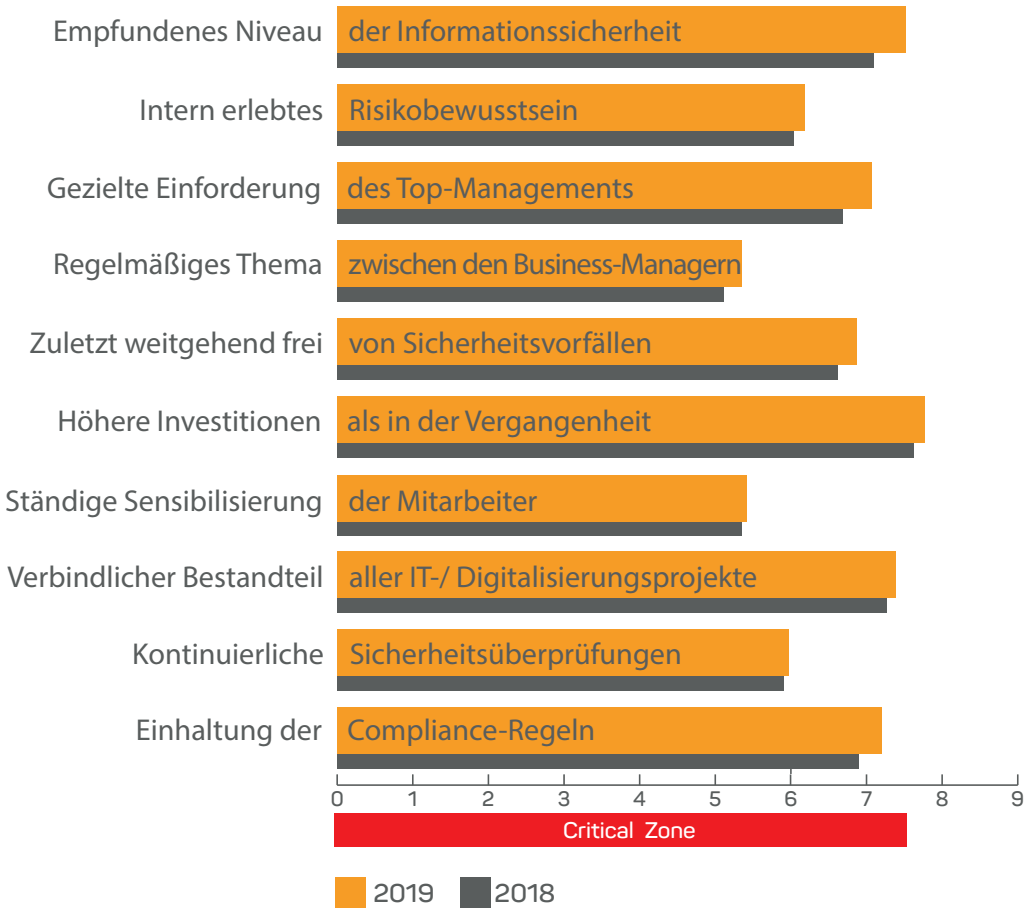
Diese Sicht scheint imMaschinenbau noch nicht recht angekommen zu sein, denn mit einem Business Information Risk-Index (BIR-I) von 66,72 gegenüber 64,60 im vergangenen Jahr ist zwar ein leichter Anstieg festzustellen. Trotzdem wird unverändert nur der sechste Platz des Branchen-Rankings eingenommen, eine Position schlechter als 2018.

So hat zwar das von den befragten Business Managern empfundene Niveau der Informationssicherheit leicht zugenommen und hat sich die Quote der registrierten Sicherheitsvorfälle leicht verbessert. Ebenso positioniert sich die Geschäftsleitung engagierter für die Informationssicherheit, aber das interne Risikobewusstsein liegt unverändert deutlich unter dem Mittelwert aller Branchen. Vor allem aber: Die Einzelergebnisse von acht der zehn Bewertungsparameter liegen in der kritischen Zone. Teilweise liegen die Unternehmen des Maschinen- und Anlagebaus auch deutlich – beispielsweise bei regelmäßigen Sicherheitsüberprüfungen - unter dem Durchschnitt aller untersuchten Branchen.

Business Information Risk Index (BIR-I)
Maschinenbau



Business Information Risk Level
Maschinenbau



CISO ALLIANCE E.V.
QUALIFIZIEREN. VERNETZEN. FÖRDERN.

Die CISO Alliance e.V. versteht sich als Berufsverband für Experten mit sicherheitsfachlichen
Aufgaben in Unternehmen, Öffentlichen Institutionen und anderen Organisationen. Sie verfolgt als primäre Ziele, das Berufsbild des CISOs weiterzuentwickeln, den Mitglieder eine Community-Plattform zu bieten sowie sie mit CISO-spezifischen Schulungen zu unterstützen. Mit der Ausrichtung „QUALIFIZIEREN. VERNETZEN. FÖRDERN." verfolgt die CISO Alliance 8 zentrale Ziele:

1. CISOs eine offene Community-Plattform bieten: Auf Basis einer facettenreichen und innovationsorientierten Fachkultur werden den Mitgliedern Zugang zu vielfältigen Partizipationsmöglichkeiten mit hohem Mehrwert für die CISO-Praxis bereit gestellt.

2. Mitwirkung bei der Etablierung einer CISO-Kompetenzkultur: Initiativen zur Entwicklung, Vereinheitlichung und Förderung des CISO-Berufsbildes, Mitgliederunterstützung bei der individuellen Definition fachlicher Qualifizierungsprofile und beim Aufbau organisatorischer CISO-Strukturen.

3. Förderung der CISO-Reputation: Systematische Impulse und Maßnahmen zur Steigerung der Wertschätzung und Anerkennung dieser Berufsgrupp, dazu gehört beispielsweise die jährliche Durchführung des CISO Award.

4. Education-Plattform für CISOs: Gezielte fachliche Förderung durch ein breites Angebot an spezifischen Schulungen und weiteren Qualifizierungs- bzw. Fortbildungsmaßnahmen.

5. Praxisorientierter Informationstransfer: Breitstellung aktueller und CISO-relevanter Informationen über Kommunikationskanäle für Mitglieder und Durchführung von Foren für den praxisbezogenen Erfahrungsaustausch.

6. Konzeption methodischer CISO-Frameworks: Gemeinsam mit wissenschaftlichen Einrichtungen und weiteren Kompetenzträgern im Markt werden Rahmenwerke entwickelt, die – auch in branchenspezifischen Versionen - das CISO-Management der Unternehmenssicherheit wirksam unterstützen.

7. Eng verzahnte Vernetzungen: Enge Zusammenarbeit mit Wirtschaftsverbänden, Branchenverbänden, fachlichen Institutionen, wissenschaftlichen Einrichtungen usw. im Rahmen einer offenen Kooperationskultur.

8. Branchenorientierte Kompetenzunterstützung: Umsetzung aller entwickelten Methoden und Standards in branchenspezifische Versionen, ebenso Durchführung branchenorientierter Arbeitsgruppen und Schulungen.

CISO ALLIANCE
QUALIFIZIEREN VERNETZEN FÖRDERN

Für Ihre Notizen:

QUALIFIZIEREN VERNETZEN FÖRDERN

CISO Alliance e.V.

Walderdorffer Hof
Fahrgasse 5
65549 Limburg

Tel. +49 6431 2196-290

- **www.ciso-alliance.de**
- Organisatorischer Kontakt
  office@ciso-alliance.de
- Mitgliederverwaltung
  mitglieder@ciso-alliance.de
- Kontakt zum Vorsitzenden
  vorsitzender@ciso-alliance.de