**„Stufen auf der Leiter zu erklimmen nützt nichts, wenn die Leiter an der falschen Wand steht.“**

Dieses Zitat von dem Managementvordenker Stephen Covey bietet einen guten Einstieg in die Notwendigkeit von Strategie und flexibler Planung.

Der Fokus der Unternehmenssicherheit liegt vor dem Hintergrund künftig zu erwartender (Sicherheits-)Risiken im Rahmen des Geschäftsbetriebs auf der Unterstützung der Unternehmensführung und Erreichung der angestrebten Geschäftsziele. Die Sicherheitsstrategie muss an der Unternehmensstrategie ausgerichtet sein um, im Rahmen der originären Unterstützungsfunktion der Sicherheitsabteilung, Präventions- und Reaktionsmaßnahmen umsetzen zu können, die ein angemessenes Sicherheitsniveau für das Unternehmen und seinen Betrieb sicherstellen.

Für die Entwicklung dieser Sicherheitsstrategie ist eine enge Zusammenarbeit zwischen Unternehmensführung und Leitung der Unternehmenssicherheit erforderlich. Die Strategie ist die Grundlage für die Steigerung der Resilienz der Organisation und bildet die Basis zu ergreifender Sicherheitsmaßnahmen und Investitionen.

Soweit der theoretische Ansatz.

> In der Praxis ist eine an die Unternehmensstrategie gekoppelte Sicherheitsstrategie hingegen äußerst selten.

Dafür gibt es 3 wesentliche Gründe:

- **Unternehmensführung fordert keine messbare Sicherheit ein**
  Da die Unternehmensführung die Verantwortung für die Sicherheit des Unternehmens trägt, ist sie in erster und letzter Instanz gefragt, eine Sicherheitsstrategie aktiv einzufordern. Zu dieser Governance-Rolle gehört auch die Zielsetzung und Kontrolle des Erreichten und damit die Überwachung der Performance des Sicherheitsmanagements und seiner Vertreter (z.B. LeiterIn Unternehmenssicherheit).

- **Keine Geschäftsstrategie als Basis**
  Begünstigt wird der Umstand, dass Unternehmen keine Sicherheitsstrategie verfolgen, dadurch, dass viele Top-Manager keine Geschäftsstrategie erstellen oder diese nicht verständlich an die Fachbereichsleitungen kommunizieren. In beiden Fällen kann grundsätzlich kein, an gemeinsamen Zielen ausgerichtetes, Vorgehen aller Abteilungen erfolgen.

- **Mangelnde Kapazitäten in der Unternehmenssicherheit**
  Viele Sicherheitsverantwortliche entwickeln, selbst wenn Unternehmensziele klar kommuniziert sind, keine Sicherheitsstrategie an der die Sicherheitsmaßnahmen, die Allokation des Budgets und die Personalauswahl sowie -weiterbildung ausgerichtet werden können.

Unabhängig dieser Gründe ist eine fehlende Sicherheitsstrategie ein Versäumnis der Beteiligten und nimmt dem Unternehmen die Grundlage für eine effektive und effiziente Unternehmenssicherheit.

Coqsecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

Die Ursachen sind zum einen mangelndes Know-How zur Entwicklung einer (Sicherheits-)Strategie und deren konsequenter Umsetzungsplanung, wenig Gehör der Sicherheitsabteilungsvertreter bei der Unternehmensführung, Zeitmangel im Tagesgeschäft und kaum Beispiele aus der Praxis die exemplarisch herangezogen werden können.

Ohne Sicherheitsstrategie und konkrete Ziele befindet sich die Abteilungsleitung der Unternehmenssicherheit, gegenüber der Unternehmensleitung und anderen Abteilungen in einer defensive Position, die es erschwert den Nutzen und die Vorteile eines entsprechenden Sicherheitsmanagements zu vermitteln. Die Darstellung der Relevanz der Sicherheit im Kontext von Zielsetzung und Wirtschaftlichkeit der Organisation, ist jedoch die Voraussetzung für die Einwerbung der notwendigen Ressourcen für die Sicherheitsabteilung und damit für deren nachhaltige Wirksamkeit.
Hinzu kommt, dass ohne Strategie die Grundlage für jegliche Argumentation zur Priorisierung und Ablehnung von, sowie der Beteiligung an Projekten fehlt und die Sicherheitsabteilung eher reaktiv getrieben statt proaktiv gestaltend tätig ist.

Damit mehr Sicherheitsverantwortliche und damit die Organisationen für die sie tätig sind, die Vorteile einer Sicherheitsstrategie und ihrer Umsetzung nutzen können, bieten wir Ihnen mit dem folgenden 4-Punkte Plan einen konkreten Leitfaden. Dieser umfasst auch die Entwicklung der operativen Umsetzungsplanung und basiert unter anderem auf Erkenntnissen und Methoden aus dem Bereich der Geschäftsstrategieentwicklung.

# 4-Punkte Plan

## für die Erstellung und Umsetzungsplanung einer zukunftsfähigen Sicherheitsstrategie

### Punkt 1 Grundlagenermittlung

Zur Erstellung der Sicherheitsstrategie sind spezifische Unternehmensdaten, insbesondere zur geplanten Entwicklung (A) und des Umfelds (B) relevant.
Die Erstellung der Sicherheitsstrategie obliegt der für Sicherheits-Governance zuständigen Stelle im Unternehmen. Diese kann die Unternehmensführung (z.B. unterstützt durch externe Sicherheitsberater) selbst oder eine dafür eingerichtete Stabsstelle Sicherheit abbilden.
An dieser Stelle sei auch auf unseren Artikel zur Relevanz der Trennung zwischen Governance & Management verwiesen (https://www.corsecon.de/_files/ugd/381794_67294c5db24846ff885988bfcf1f4079.pdf ).

**A – Identifizierung der Kernpunkte der Geschäftsstrategie**
Nach Möglichkeit wird die ausformulierte Geschäftsstrategie als Grundlage für die Sicherheitsstrategie herangezogen. Ist keine verfügbar, eignen sich Interviews mit der Unternehmensführung um die, für die Sicherheitsstrategie relevanten Aspekte (Geschäftsmodell, -entwicklung), zu ermitteln. Von besonderem Interesse sind die folgenden Punkte:

- Neue (digitale) Geschäftsmodelle
  Sie konfrontieren die Sicherheitsorganisation mit individuellen Anforderungen (neue Angriffsformen und -vektoren). Dafür ist entsprechendes Know-How (u.a. Threat Intelligence) aufzubauen und die, meist getrennt arbeitenden, Abteilungen IT(-Sicherheit) und Unternehmenssicherheit zu konsolidieren bzw. enger zu verzahnen.

- Einsatz neuer Technologien an Standorten
  Der Umstieg auf neue Technologien (PV-Anlagen, Umstellung der Fahrzeugflotte auf E-Fahrzeuge, Nutzung von Drohnen) macht u.a. Anpassungen im vorbeugenden Brandschutz, der Arbeitssicherheit und Notfallorganisation (z.B. Quarantänefläche für verunfallte E-Fahrzeuge) erforderlich.

- Industrie 4.0 (autonome Produktion)
  Sie erfordert beispielsweise, zusätzlich zum bisherigen Objektschutz, die Absicherung der notwendigen IT-Infrastrukturen und Beschäftigung mit Non-Cyber Informationssicherheit (digitale Zwillinge, Fernsteuerung sowie Fernwartung der Systeme).

- Internationalisierung des Geschäfts
  Ein geplanter Markteintritt in fremde Länder stellt neue Herausforderungen an die Standort- und Reisesicherheit. Länderspezifische Gesetze zu Sicherheitsmaßnahmen und eine andere Sicherheitskultur erfordern eine Anpassung gängiger Sicherheitsmaßnahmen. Dazu zählen Änderungen in der Struktur der Sicherheitsorganisation (zusätzliches Personal o. Leitstand, Anpassung und Übersetzung von Richtlinien) als auch in den Sicherheitsprozessen (z.B. Krisenmanagement).

- Geplante Neu- und Umbauten
  Bauliche Veränderungen in der Betriebsorganisation z.B. die Einrichtung von Kundenservicecentern oder innovativen Ladengeschäft-Konzepten verändern die Anforderungen an die Sicherheitsorganisation. Sie bilden die Ausgangspunkte für Sicherheits- und Schulungsmaßnahmen sowie den Einsatz geeigneter Sicherheitstechnik und -software.

- Zukäufe und Restrukturierungen
  Die Zusammenführung der Sicherheitsabteilungen und -strukturen mehrerer Unternehmen ist anspruchsvoll und erfordert ein eigenes Konzept.

Corsecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

**B – Analyse der Risikolandschaft und Gefährdungslage des Unternehmens**
Die Auswertung von verfügbaren Daten zu Risiken (allgemeinen Gefahren) im Bereich Safety, Security, IT-Security und Details zu Tätergruppierungen bzw. deren Verhalten mit dem Ziel der individuellen Informationsgewinnung werden unter dem Begriff Business Security Intelligence zusammengefasst.

Relevante Daten für eine Auswertung sind:
- Kriminalitätsstatistiken und Daten von (Sach-)Versicherern
- Geplante neue Gesetze oder Gesetzesänderungen, die zu mehr Regulierung führen: u.a. geplantes Gesetz zur Unternehmenshaftung, Hinweisgeberschutzgesetz oder KRITIS-Dachgesetz
- Hinweise zu aufkommenden neuen oder sich verschärfenden Risiken wie z.B. Stromausfallszenarien oder Umweltkatastrophen
- Geänderte Bedrohungslage durch Dritte, z.B. neue Kriminalitätsfelder und -phänomene wie u.a. Verlagerungen im Bereich Cyberkriminalität, hin zu vermehrt staatlichen Akteuren bei Cyberangriffen, Spionage und Desinformationskampagnen
- Professionalisierung von Tätern (Organisierte Kriminalität und Cyberangriffe als buchbare Dienstleistung)
- Neue Geschäftsmodelle (Double Extortion bei Cyberangriffen, Whaling, Smishing, …)

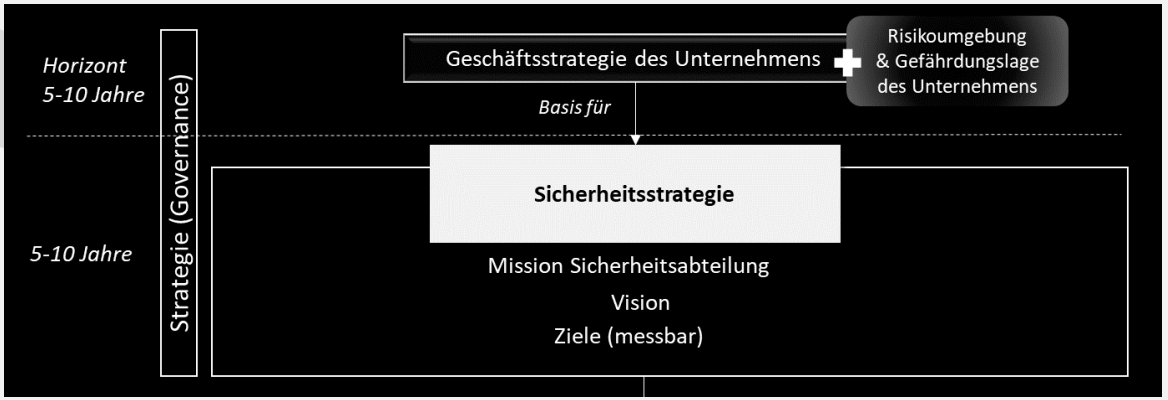
- Einsatz neuer Technologien (u.a. KI für Deep Fakes, Einsatz von Drohnen zum Ausspähen/Abhören und Einbringen von Gegenständen, Einsatz von Oberflächen (z.B. Mänteln), die Personen und Objekte für Augen und Kameras unsichtbar machen –> kennen Sie schon Quantum Stealth ?)
- Zukunftsforschung: Megatrend Sicherheit (siehe Corsecon-Fachartikel)

Die anschließende Prüfung, welche Risiken aktuell und in Zukunft (B), im Rahmen der geplanten Entwicklung des Unternehmens (A), auf Sicherheitslücken (Schwachstellen physischer oder organisatorischer Art) im Unternehmen treffen, ergibt die tatsächlich zu behandelnden Gefährdungen.
Die Gefährdungen wirken sich, in Form von Personenschäden, Haftungsrisiken, Betriebsunterbrechungen und finanziellen Schäden aus und beeinflussen damit die Geschäftsziele negativ.

Eine Annäherung an die Schadenhöhe, ohne Investitionen in die Unternehmenssicherheit, ermöglicht die Betrachtung des Risikopotentials (Eintrittswahrscheinlichkeit und Schadenausmaß).
Aus diesen Erkenntnissen lassen sich die grundsätzlich notwendigen Anpassungen in der Sicherheitsorganisation antizipieren und vornehmen.
Die potentielle Schadenhöhe von Ereignissen, ohne unternehmerische Sicherheitsvorkehrungen, bildet die Grundlage für die Berechnung der Wirtschaftlichkeit von Sicherheitsmaßnahmen und dem Unterhalt der Sicherheitsorganisation.
Dieser Wert muss vom Budgetgeber (Unternehmensführung) verifiziert und ins Verhältnis zu den erwarteten Geschäftsergebnissen, durch die Erreichung der Ziele im Rahmen der Geschäftsstrategie, gesetzt werden.

## Punkt 2
## Sicherheitsstrategie formulieren

Eine Strategie gibt einen, zeitlich längerfristig (5-10 Jahre) angelegten definierten, Rahmen für ein Unternehmen oder einen Bereich vor, indem ein gewisser Zustand hergestellt werden soll, der sich anhand konkreter Ziele (quantitativ & qualitativ: Umsatz, Reichweite, Kundenanzahl) bemessen lässt. Die Inhalte der Strategie, im Bereich Mission, Vision und Ziele vermitteln, neben der Langfristigkeit der Ausrichtung,




gleichzeitig die Ambition des Unternehmens. Exemplarisch wird im Folgenden die Formulierung der Strategie sowie die Entwicklung der strategischen und operativen Planung anhand eines Automobilherstellers skizziert, dessen Gesamtunternehmensstrategie die Entwicklung zu einem Mobilitätskonzern ist.

- Mission: Mobilität für Alle
- Vision: Jeder weltweit gelangt zu jeder Zeit an sein Ziel.
  (Die Vision wird so ambitioniert formuliert, dass sie nicht vollständig erreicht werden kann, dies erfordert stetige Verbesserung und motiviert die Beteiligten.)
- Ziele:
  - X aktive Nutzer der Mobilitätsangebote & Services (Charter-Flüge für Kurzstrecken, Car Sharing, autonome Taxis Schaffung einer App zur Buchung von Mobilitätsleistungenanderer Partner (z.B. Bahn)
  - Investoren gewinnen (X Euro), X Euro Umsatz
  - Schaffung X Arbeitsplätze in EMEA-Region
  - > 80 % der Nutzer fühlen sich „sehr sicher“ bei Transfers
  - durchschnittliche Transferkosten für Nutzer unter 50 Euro senken

Die daraus abgeleitete Sicherheitsstrategie für die Abteilung Unternehmenssicherheit könnte wie folgt aussehen:

**Sicherheitsstrategie**

- Mission (Abteilungszweck): Unterstützungsfunktion für Kerngeschäft
  - Geschäftsbetrieb absichern (Kernmission)
  - Sicherheit als USP, im Rahmen des Geschäftsmodells, für das Unternehmen etablieren (Mehrwert Wettbewerbsvorteil und Wertschöpfung)

- Vision (Angestrebter Zustand)
  (Ausfall-)sichere Mobilität
    - Null Personenschäden (physisch & psychisch) im Geschäftsbetrieb (Kunden, Dienstleister, Personal)
    - keine Serviceausfälle für Endkunden
- Ziel (Gewünschtes Ergebnis):
  Schadenminimierung
    - <10 Tote und <150 Schwerverletzte weltweit, im Rahmen von Unfällen im Geschäftsbetrieb unter Mitarbeitern oder Kunden
    - Keine Haftungsfälle im Top-Management und Schadenersatzzahlungen unter X Euro halten
    - kostenintensive Betriebsunterbrechungen vermeiden (< X € und < X Zeitraum Serviceausfälle pro Jahr pro Kunde)
    - Öffentlich gelungen wahrgenommene Krisenkommunikation zum Schutz der Reputation im Fall von Sicherheitslecks/Vorfällen (qualitatives Ziel)
    - Sicherheitsgefühl „sehr sicher“ bei > 80 % der Nutzer über alle Verkehrsmittel hinweg
    - Weitere Ziele im Rahmen des klassischen Sicherheitsmanagements und gesetzlicher Vorgaben (Reduktion von Sicherheitslücken, Einbrüchen, Arbeitsunfällen, Schulungen für Stäbe, Rollouts…)

Eine so entwickelte Sicherheitsstrategie zahlt mit ihren Ergebnissen auf die Ziele der Geschäftsstrategie der Unternehmensführung ein, indem sie unternehmensweite Projekte ermöglicht oder absichert. Die offizielle Genehmigung und Unterstützung sowie Bereitstellung des erforderlichen Budgets durch die Unternehmensführung wird dadurch sehr wahrscheinlich und muss eingefordert werden.
An der beschriebenen und übergeordneten Sicherheitsstrategie (Mission, Vision und Ziel) orientiert sich die gesamte strategische und operative Sicherheitsplanung. Sie sorgt für die notwendige Flexibilität des Unternehmens bei der Verfolgung der strategischen Ziele. Äußeren Einflüsse kann durch flexible Planungen von Projekten und Steuerung von Einzelmaßnahmen innerhalb von Initiativen angemessen begegnet werden. Zudem können auf dieser Ebene gesetzte Ziele bei der Erreichung nach oben angepasst werden.

## Punkt 3
## Strategische Planung

Zur Differenzierung und Detailplanung einzelner Vorhaben, die mit ihren Ergebnissen auf die Erreichung der Strategieziele einzahlen, hilft die Festlegung von Initiativen. Sie lenken den Fokus und Einsatz der Ressourcen der Unternehmenssicherheit.
Der Aktionsplan setzt sich aus den Initiativen (Themenschwerpunkten) zusammen, die die Erreichung der strategischen Ziele sicherstellen. Dazu können zwischen 5 und 10 Initiativen, je nach Abteilungsgröße, definiert werden.
Die Entwicklung und Steuerung des Plans obliegt, in Abgrenzung zur Sicherheitsstrategie der für Governance zuständigen Stelle, der Leitung der Sicherheitsabteilung bzw. dem Sicherheitsmanagement.

**Aktionsplan**
Zielsetzung

1. Initiative „Ansprechpartner Sicherheit“
   Sicherheitsberatung & Notfallsupport für Geschäftseinheiten und Endkunden

2. Initiative „Sicherheits-Weiterbildung“
   Steigerung der Awareness und Aufbau von dezentraler Sicherheitskompetenz durch Qualifizierung von Kunden, Partnern und Mitarbeitern.

3. Initiative „Digitalisierung der Sicherheitsorganisation“
   Digitalisierung der Sicherheitsprozesse und -maßnahmen, insbesondere im Bedrohungsmanagement.

4. Initiative „Abteilungsfusion IT- und Unternehmens-sicherheit“
   Zusammenführung der Abteilungen IT-Sicherheit und Unternehmenssicherheit (enge Zusammenarbeit bei Risikomanagement, Betrugsfällen, Ransomware, Sabotage)

Coqsecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

**Messwerte und Metriken**
Um die Fortschritte bei der Zielerreichung zu überwachen ist die Datensammlung und Festlegung konkreter Messwerte (quantitativ und qualitativ) sowie Benchmarks notwendig.

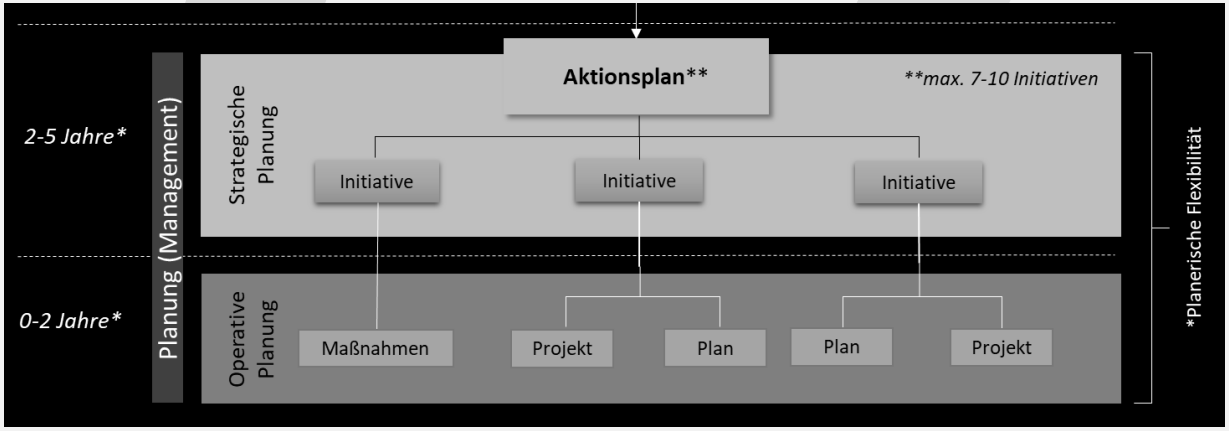
- Kundenbewertungen zu Sicherheitsgefühl
- Unfallstatistiken (Opfer, Verursacher)
- Statistik der (Arbeits-)Unfälle (Psych./Phys. Gewalt ggü. Fahrern und Servicemitarbeitern)
- Anzahl geschulter Mitarbeiter zu Risiken & Sicherheitsmaßnahmen durch Sicherheitsabteilung und Multiplikatoren
- Angenommene Anrufe an der Notfallhotline (Kunden und Servicepartner)
- Erfasste Betrugsdelikte (Kunden / MA) sowie Schadenstatistik und Trendgraph
- Anzahl digitalisierter Prozesse und lizensierter Software
- Anzahl negativer Presseberichte zum Thema Kundensicherheit, unterteilt nach Regionen und Medienreichweite
- Die, zur Umsetzung der Initiativen erforderlichen, Projekte und Einzelmaßnahmen werden innerhalb der operativen Planung vorbereitet und umgesetzt.

## Punkt 4
## Operative Planung vornehmen

Ziel der operativen Planung ist die Auswahl geeigneter, konkreter Maßnahmen und Projekte, die der Erreichung der übergeordneten gesetzten Ziele dienen. Dazu werden sowohl technische, organisatorische als auch personelle Maßnahmen ergriffen.

Der bisher beschriebene Aufbau von Strategie und Planung ermöglicht der Sicherheitsabteilung transparent begründbare Entscheidungen in welche Projekte anderer Abteilungen die Mitarbeiter eingebunden werden sollten und welche Maßnahmen eigeninitiiert umgesetzt werden.
Auf dieser Basis ist die Unternehmenssicherheit weit weniger getrieben von den, meist spontanen und oft überbordenden, Anforderungen (Zeit, Unterstützung) anderer Abteilungen, da auch die Ablehnung von Projekten, zugunsten der Verfolgung der mit der Unternehmensführung abgestimmten übergeordneten Ziele aus der Sicherheitsstrategie, legitim wird.

Das Sicherheitsmanagement agiert damit im Unternehmenskosmos proaktiv.
So verfolgt die Unternehmenssicherheit transparent und konsequent die eigene Agenda, was die Voraussetzung für die Erreichung der




Sicherheitsziele des Unternehmens ist.
Umsetzungspläne und Projekte

1. Projekte und Maßnahmen der Initiative „Ansprechpartner Sicherheit“
- Zentrales digitales Vorfalltracking (Notfallbutton in Fahrzeugen, Sturzsensoren bei Rollern und Button in Kunden-App)
- Übernahme von Ermittlungen (Hinweisgebersystem)
- Initiierung Meldebutton in App zur Meldung von Sicherheitsmängeln und Beinahe-Unfällen (Unfallverhütung & Prävention)
- Initiierung einer Notfallzentrale für Kunden
- Veröffentlichung Leitfaden zur Due Diligence bei Servicepartnern (Vorstrafen Fahrer usw.)

2. Projekte und Maßnahmen der Initiative „Sicherheits-Weiterbildung“
- Weiterbildung im Bereich Mobilität & neue Technologien für Mitarbeiter der Unternehmenssicherheit, des Brandschutzes und der Arbeitssicherheit (inkl. neuer Risiken z.B. Feststoffbatterien, Standorte der Zukunft, eingesetzte Systeme IT und Schnittstellen, Anpassung BCM für neue Geschäftsmodelle und -bereiche (u.a. IT))
- Krisenkommunikationsschulungen für Unternehmenskommunikationsabteilung und Geschäftseinheiten
- Visualisierung der Sicherheitshinweise für Kunden (Safety & Security) anstelle Textdokumente
- Sicherheitsschulungen (Deeskalation usw.) für Personal an Service- und Ausgabepunkten durchführen

3. Projekte und Maßnahmen der Initiative „Digitalisierung der Sicherheitsorganisation“
- Ticketsystem einrichten
- Einrichtung digitaler Notfallstabsräume
- Zentrales Monitoring und Bewertungsplattform für Bedrohungen
- Betrugsprävention durch Schulungen der Führungskräfte Ebene 3 und höher
- Einbindung von KI zur Früherkennung von Sicherheitsvorfällen im Straßenverkehr international

Corsecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

4. Projekte und Maßnahmen der Initiative „Abteilungsfusion IT- und Unternehmenssicherheit“
- Personalplanung
- Abteilungsbeschreibung
- Teambuilding
- Prozessangleichung
- Abstimmung Incident Response Teams (IT) und Notfallmanager

Die notwendige Flexibilität bei der Umsetzung der Sicherheitsstrategie, in der heutigen VUCA-Welt mit den sich ständig ändernden Bedingungen, bietet die strategische und insbesondere die operative Planung.
Sie ermöglicht sowohl die vorzeitige Beendigung von Projekten aufgrund veränderter Gegebenheiten, als auch die Setzung höherer Ziele nach der Erreichung der ursprünglich gesetzten.

Das beschriebene systematische Vorgehen zu Sicherheitsstrategie und Planung ermöglicht zum einen die konsequente Verfolgung übergeordneter, an denen des Unternehmens ausgerichteter, Strategieziele und bietet dabei zum anderen die im Alltag notwendige Spielräume für flexibles Sicherheitsmanagement der Abteilung Unternehmenssicherheit.

Quellen: Gartner, HBM, Corsecon

# Sicherheitsstrategie & -planung

Coresecon
AGENTUR FÜR SICHERHEITSMANAGEMENT

**Differenzierung zwischen Strategie & Plänen**

Horizont 5-10 Jahre

Strategie (Governance)

Geschäftsstrategie des Unternehmens + Risikoumgebung & Gefährdungslage des Unternehmens

*Basis für*

5-10 Jahre

**Sicherheitsstrategie**

Mission Sicherheitsabteilung

Vision

Ziele (messbar)

2-5 Jahre*

Planung (Management)

Strategische Planung

**Aktionsplan****

***max. 7-10 Initiativen*

Initiative | Initiative | Initiative

0-2 Jahre*

Operative Planung

Maßnahmen | Projekt | Plan | Plan | Projekt

*Planerische Flexibilität