excepture

Business Interface Management

Schwierigkeiten der Risikokommunikation

Ein Erklärungsversuch, warum sich viele Unternehmen schwer tun, systematisch IT-Risiken zu benennen.

Workshop der Fachgruppe SECMGT, 10.06.2016, Frankfurt a.M.

Referentin: Kirsten Messer-Schmidt

Kirsten Messer-Schmidt

- Managing Director der Firma excepture in Bonn
- Senior Consultant / Business Coach mit den Schwerpunkten: Governance, Risk, Compliance, Information Security und Kommunikationsmanagement

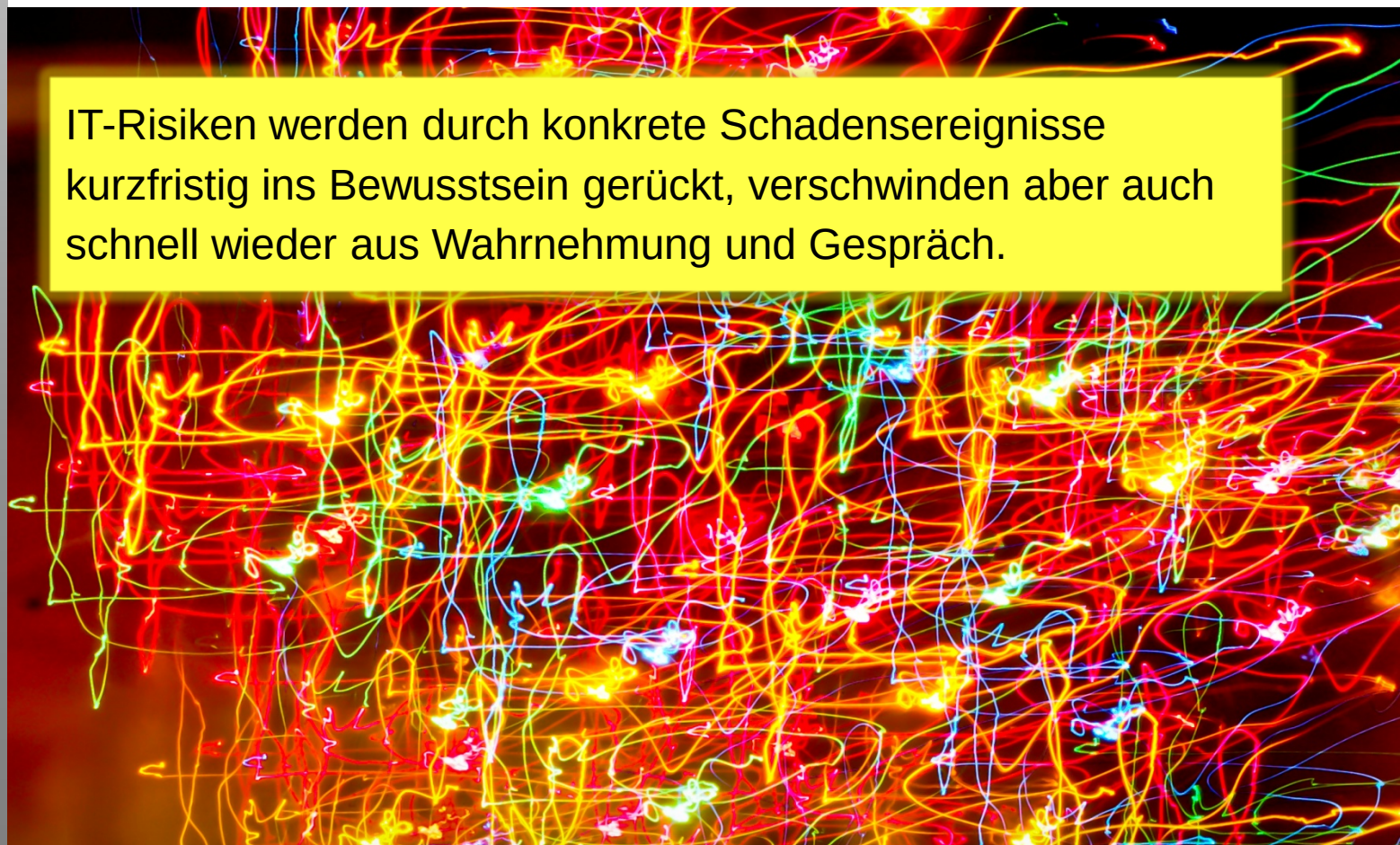
- Senior Expertin ISO 27001:2013, IT-Grundschutz
- Lead Auditor ISO 22301
- Risk Manager (TÜV)
- PRINCE2 Practitioner, Scrum Master
- Zertifizierte Personal Coach (ITT/Universität Bielefeld)

- Sprecherin des Arbeitskreises „Kritische Informations- und Kommunikationsinfrastrukturen“, GI
- Mitglied des Leitungsgremiums der Fachgruppe Management für Informationssicherheit, GI
- Mitglied des Prüfungsausschuss für IT-Strategic/Operative Professionals der IHK Köln

Zustand

Zustand der IT-Risikokommunikation

Trotz der elementaren Bedeutung von ITK für Unternehmen und den potenziell bestandsgefährdenden Auswirkungen von IT-Störungen, stößt der Versuch, IT-Risiken systematisch zu kommunizieren, häufig auf Unbehagen und Abwehr.



IT-Risiken werden durch konkrete Schadensereignisse kurzfristig ins Bewusstsein gerückt, verschwinden aber auch schnell wieder aus Wahrnehmung und Gespräch.

… und Compliance ?

Der schwache Zustand der Risikokommunikation erstaunt umso mehr, als viele Unternehmen aufgrund ihrer Branchenzugehörigkeit oder ihrer Rolle als Dienstleister

- gesetzlich und/oder vertraglich verpflichtet sind, Risikomanagement zu betreiben,
- oder sich selbst dazu verpflichtet haben.

Relevante Gesetze, Vorgaben, Normen und Standards:

- gesetzliche und regulatorische Vorgaben wie z.B. MaRisk für Banken
- ISO 27001, IT-Grundschutz, ISO 22301, ISAE 3402, IDW PS 951 n.F.
- mittelbar auch ITIL und CMMI

Risikokommunikation nach ISO 31000

ISO 31000

Risk communication and consultation: continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage **in dialogue** with stakeholders regarding the management of risk.

ISO 27005:2011

Information security risk communication and consultation:

[…] Communication will ensure that those responsible for implementing risk management, and those with a vested interest understand the basis on which decisions are made and why particular actions are required. **Communication is bi-directional.**

Formalisierung ersetzt Dialog

Einsame Papierübungen und Risikobewertungen ersetzen den Austausch zwischen verschiedenen Stakeholdern, z.B.

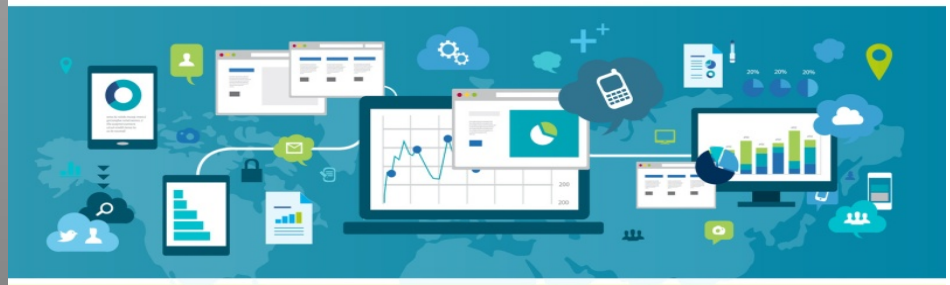
- Ablaufbeschreibungen zum Risikomanagement,
- komplizierte Berechnungsmodelle,
- Formulare, z.B. für Change Requests und Projektanträge,
- Kennzahlen,
- Restrisiko-Deklarationen.

… und sind beschränkt auf Teilbereiche der IT.

ITK ist überall: Komplexität und Vielfalt von IT-Risiken

Die Fülle von Einsatzbereichen von IT-Systemen, der hohe Vernetzungsgrad und die große Zahl verschiedener Stakeholder, machen es schwer:

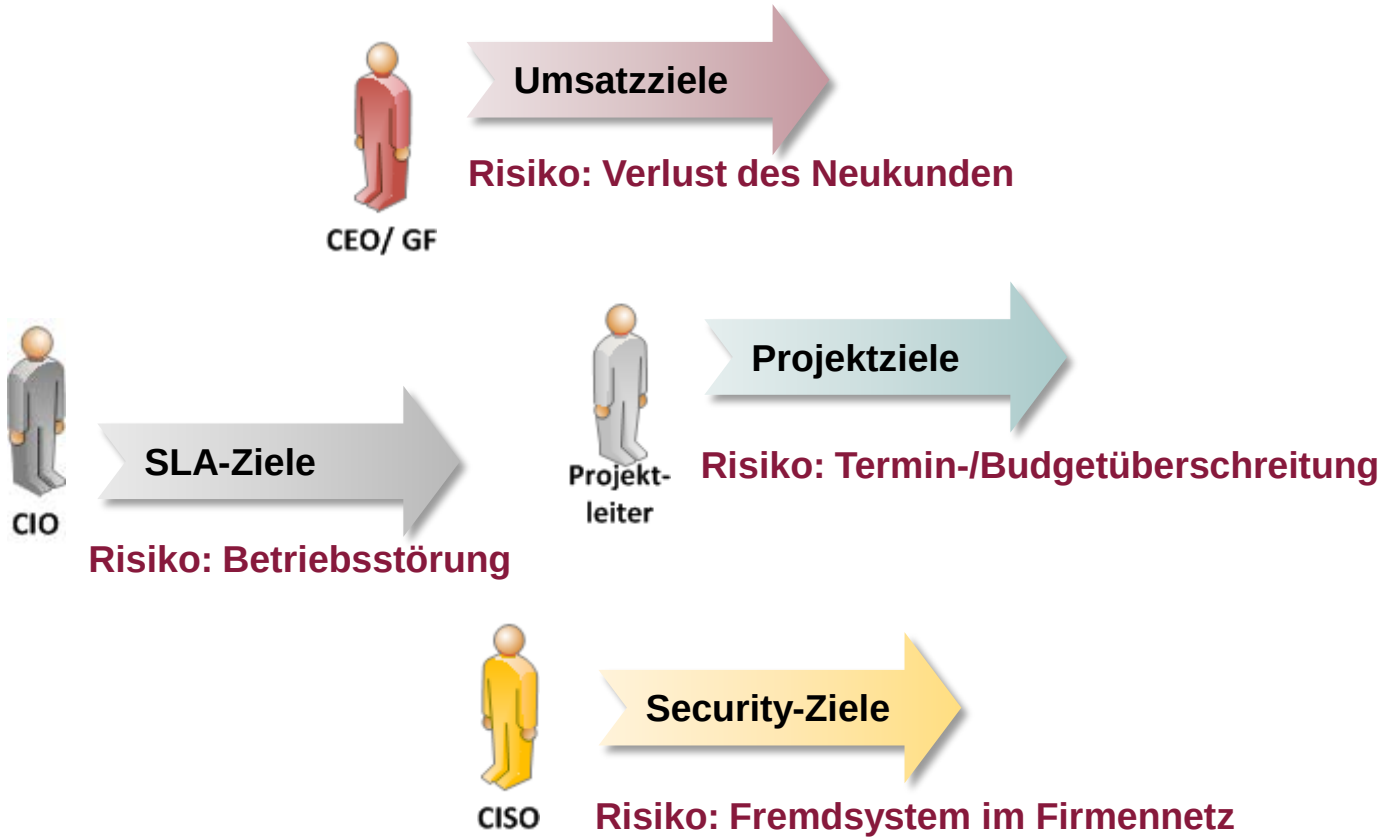
- den Scope geschäftsrelevanter IT-Risiken zu bestimmen,
- eine gemeinsame Sprache für die Beschreibung von IT-Risiken zu finden,



… und dann gibt es auch noch Risiko-Tabu-Zonen!

Unterschiedliche Ziele und Risikowahrnehmung

… ein Beispiel: Unternehmen Alpha hat einen großvolumigen Kundenauftrag für die Erbringung von Managed Services gewonnen, für den jedoch Zugeständnisse bezogen auf interne Vorgaben, Technologien und IT-Sicherheitsstandards gemacht werden müssen.



Kultur

Fehlende Risikokultur erschwert Risikokommunikation

- fehlende Vereinbarungen zur Risikobereitschaft und zur Bewertung von Risiken,
- nicht definierte Kommunikationswege,
- mangelnde Wertschätzung der Risikoüberbringer - der „hysterische“ Sicherheitsbeauftragte als Show Stopper

Macher-Kulturen und optimistische Verzerrung

Eine fehlende Risikokultur in Unternehmen findet sich häufig in „Macher“-Kulturen.

- Macher-Kulturen sind geprägt von
  - einer über-optimistischen Einschätzung der eigenen Handlungs- und Reaktionsfähigkeit,
  - der Illusion von Kontrolle.
- Es gilt als Zeichen von Schwäche, über Risiken – also Unsicherheiten – zu sprechen (Beschädigung des eigenen Experten-Images).

Spielverderber

Spielverderber-Effekt bei „Technikspielzeugen“

… noch ein Beispiel: Der Vertriebsdirektor eines Unternehmens erfährt von einem erfolgreichen Kollegen von einer neuen CRM-Software, mit deren Unterstützung die Kundenakquise deutlich besser wird. Einwand des CISO, das System wird in einer US-amerikanischen Cloud betrieben und kann daher nicht eingesetzt werden.

Affektheuristik und IT

Die Einschätzung von Risiko und Nutzen ist abhängig von der Einstellung zu einer Technologie.

„Wenn Personen eine positive Einstellungen zu einer Technologie haben, schreiben sie ihr einen großen Nutzen und ein geringes Risiko zu und umgekehrt.“*

* Daniel Kahnemann: Thinking, fast and slow

Angst

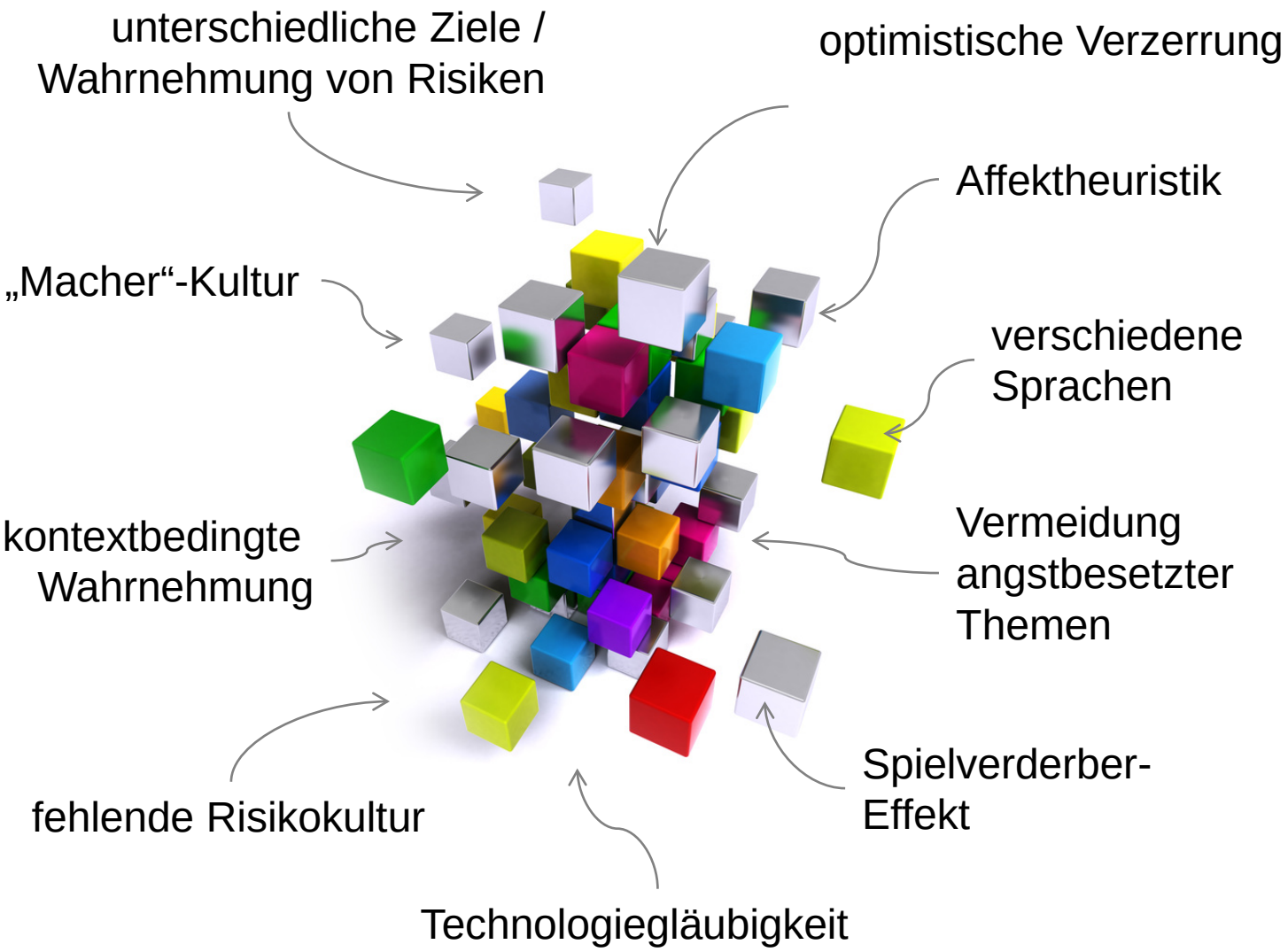
Vermeidung angstbesetzter Themen / Technologieglaube

Über IT-Risiken sprechen und sie einschätzen, heißt auch die Möglichkeit in Erwägung zu ziehen,

- dass es schon Schadensereignisse gegeben hat,
- dass möglicherweise Hilflosigkeit bezüglich erforderlicher Maßnahmen besteht,
- dass Technologie nicht grundsätzlich beherrschbar und berechenbar ist,
- dass man es vielleicht nicht im Griff hat.

… steht im Widerspruch zur Technologiegläubigkeit und dem verbreiteten Glauben an die Verlässlichkeit von IT-Systemen.

Stolpersteine



Ausblick

Danke !

excepture
Kirsten Messer-Schmidt – Managing Director / Consultant

Franzstr. 9 | 53111 Bonn
Phone: 0228 18031040 | Mail: info@excepture.de

Bildrechte

Folie 3, 10, 13	© gratisography, Ryan McGuire
Folie 7	© fotolia , Julien Eichinger
Folie 9	© fotolia, alphaspirit
Folie 11	© fotolia, pholidito
Folie 12	© fotolia, Sergey Nivens
Folie 14	© fotolia, Franck Boston
Folie 15	© fotolia, olly