



# Der Cyberschaden aus Sicht der Versicherung

Michael Guiao/ AXA Konzern AG / Kompetenzstelle Cyber  
08. – 09.10.2019 - Nürnberg

# Inhalt

## it-sa | Der Cyberschaden aus Sicht der Versicherung

1. Einleitung
2. Bedrohungslage
3. Schadenbeispiele
4. Cyber Risk Assessment
5. AXA Cyber „Öko-System“
6. Fazit & Diskussion





# 2

## Bedrohungslage

# Bedrohungslage

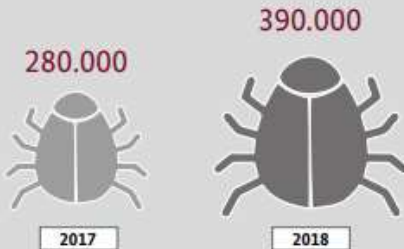
## Erkenntnisse aus dem BSI-Lagebericht 2018

### BEDROHUNGEN IM NETZ

#### Schadprogramme im Umlauf



#### Neue Schadprogramm-Varianten pro Tag

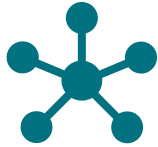


### FOKUS DER ANGRIFFE WIRD BREITER



# Bedrohungslage

## Entwicklung



- Vernetzung nimmt zu - Geräte und Systeme sind vernetzt, online verfügbar und können sogar ferngesteuert werden.



- Cyber-Kriminalität steigt: Angreifer öffnen sich immer mehr Wege, um Systeme und Netzwerke anzugreifen.



- Fehlende Sicherheit und Risikobewusstsein bei vielen Unternehmen



# 3 Schadenbeispiele

# Schadenbeispiele

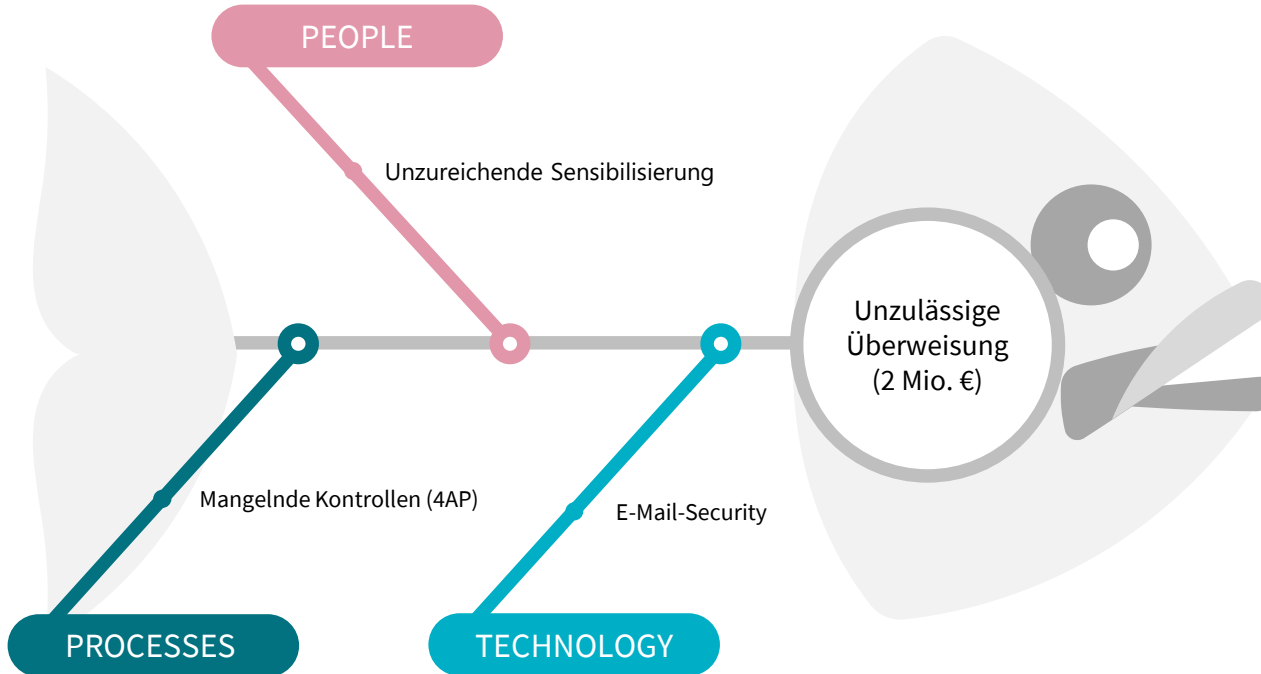
Worüber sollen wir reden?



# Schadenbeispiele

## Schadenszenario: CEO-Fraud / Social Engineering

Ursache → Auswirkung → Folgen



Folge	Kosten
Unzulässige Zahlung	2.000.000 €
IT-Analyse und Dekontamination (IT-Forensik)	80.000 €
Krisenkommunikation	2.000 €
<b>Schadenhöhe</b>	<b>Ca. 2.100.000 €</b>

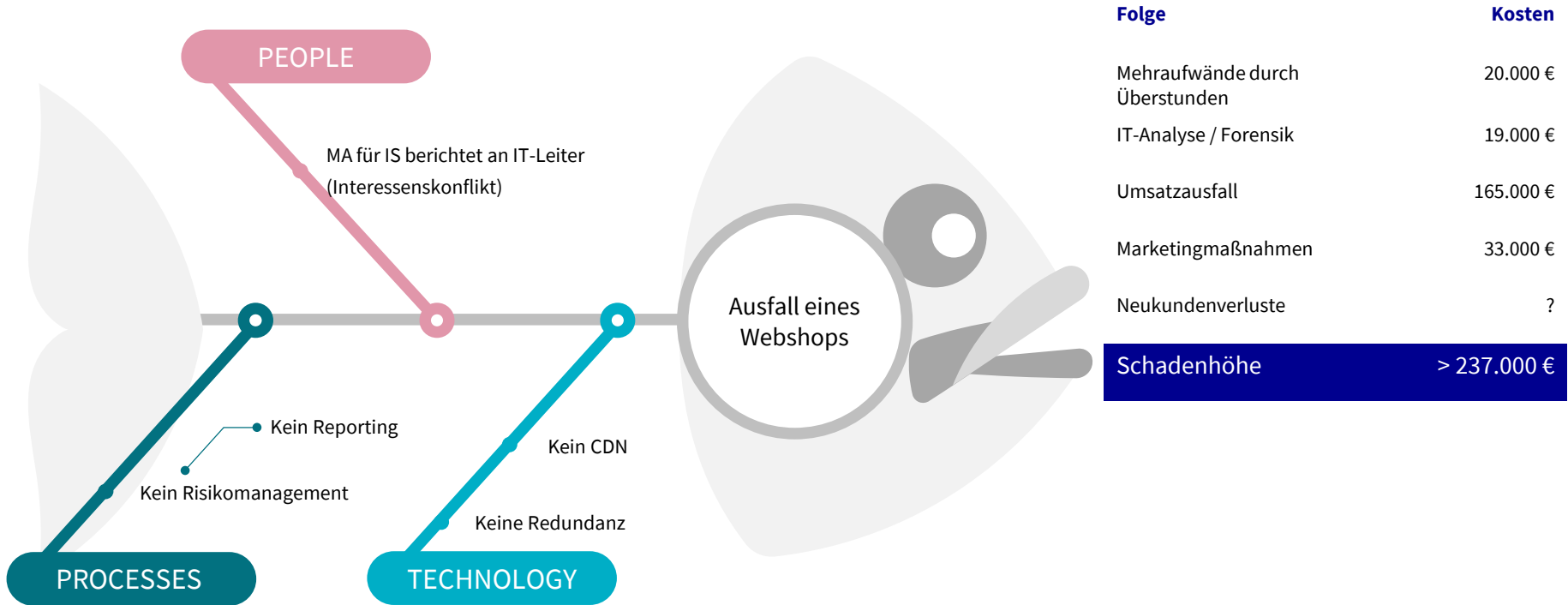




# Schadenbeispiele

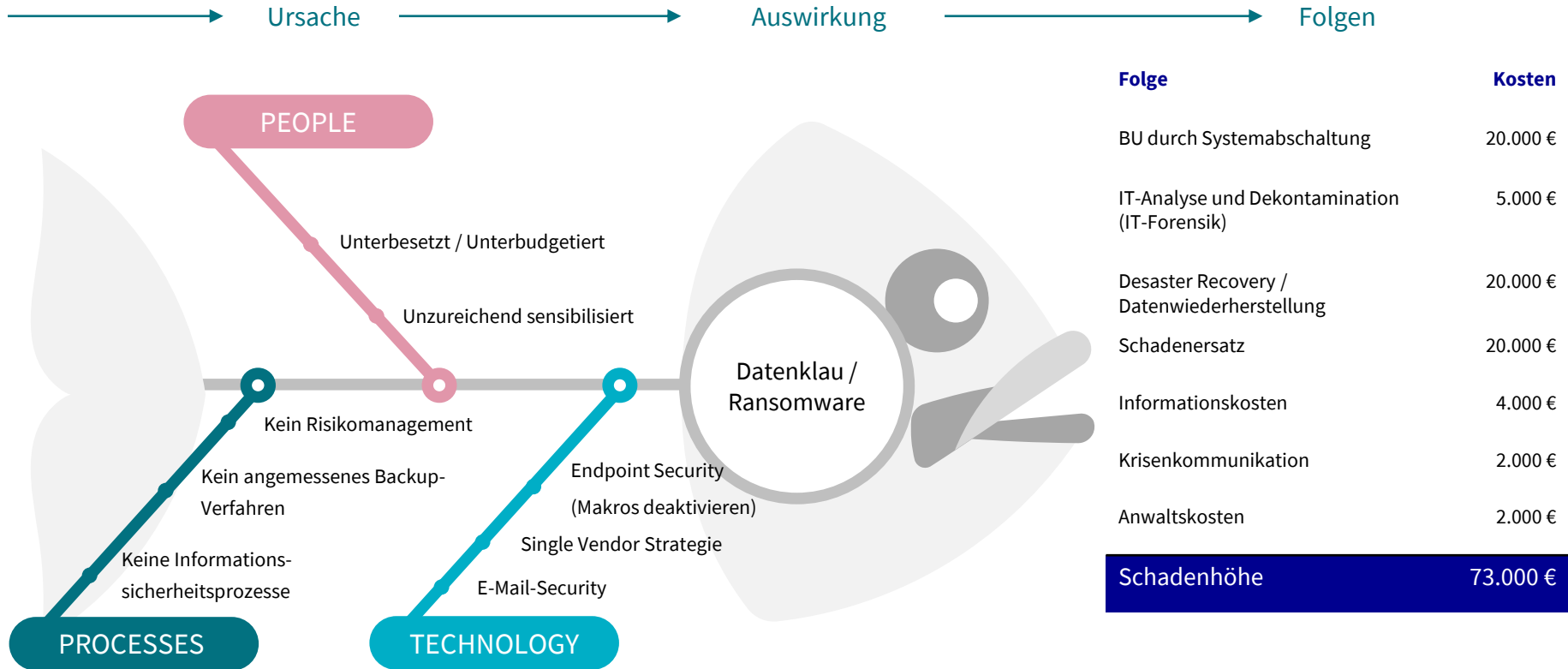
## Schadenszenario: Ausfall eines Webshops (DoS-Angriff)

Ursache → Auswirkung → Folgen



# Schadenbeispiele

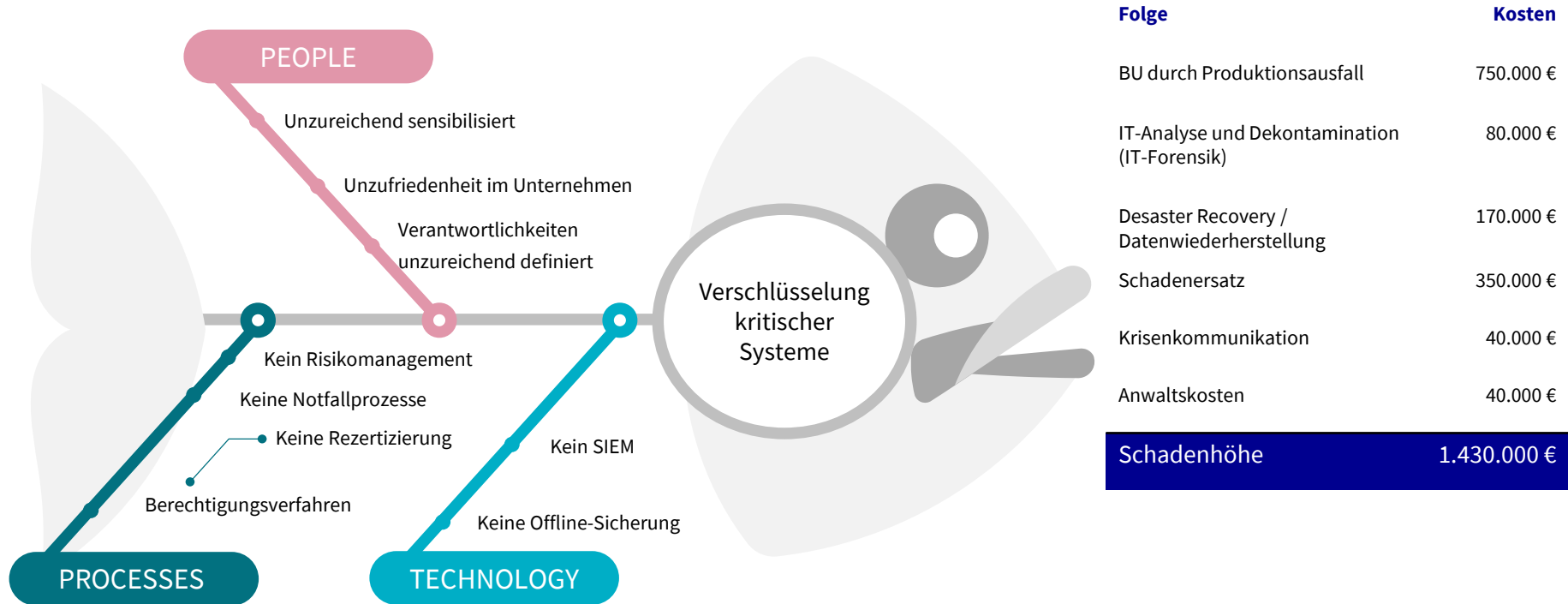
## Schadenszenario: Datenschutzvorfall in einer Arztpraxis



# Schadenbeispiele

## Schadenszenario: Verschlüsselung kritischer Systeme in der Produktion

Ursache → Auswirkung → Folgen

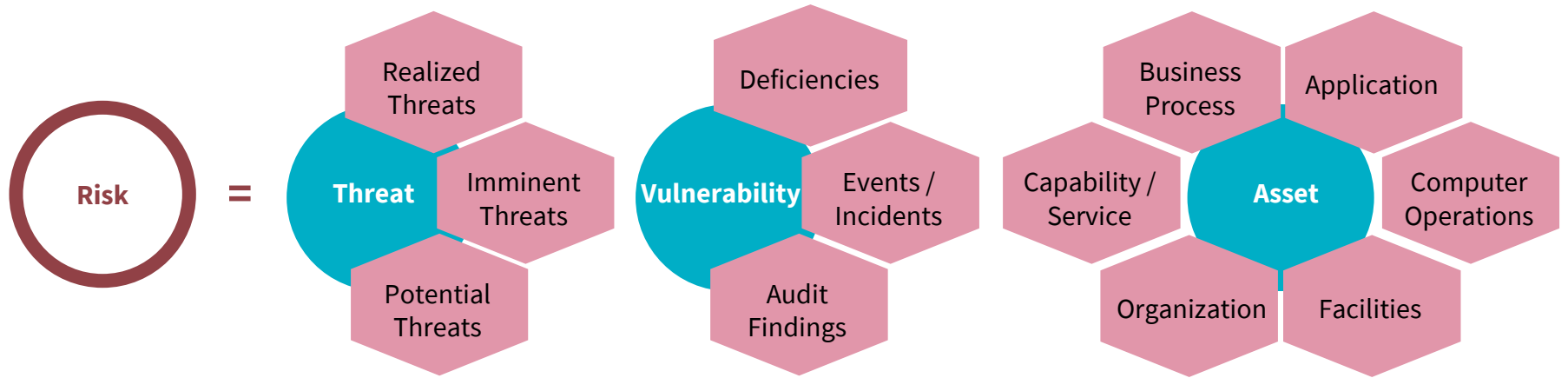




# 4 Cyber Risk Assessment

# Cyber Risk Assessment

## Risikoverständnis



# Cyber Risk Assessment

## Cyber Security Management Fähigkeiten

### Identify

Entwicklung eines organisatorischen Verständnisses um Cyber-Risiken zu managen.

### Protect

Entwicklung und Etablierung angemessener Maßnahmen, um die Verfügbarkeit, Integrität und Vertraulichkeit kritischer Services sicherzustellen.

### Detect

Entwicklung und Etablierung angemessener Aktivitäten, um Cyber-Ereignisse zu identifizieren.

### Respond

Entwicklung und Etablierung angemessener Aktivitäten, um auf Cyber-Ereignisse zu reagieren.

### Recover

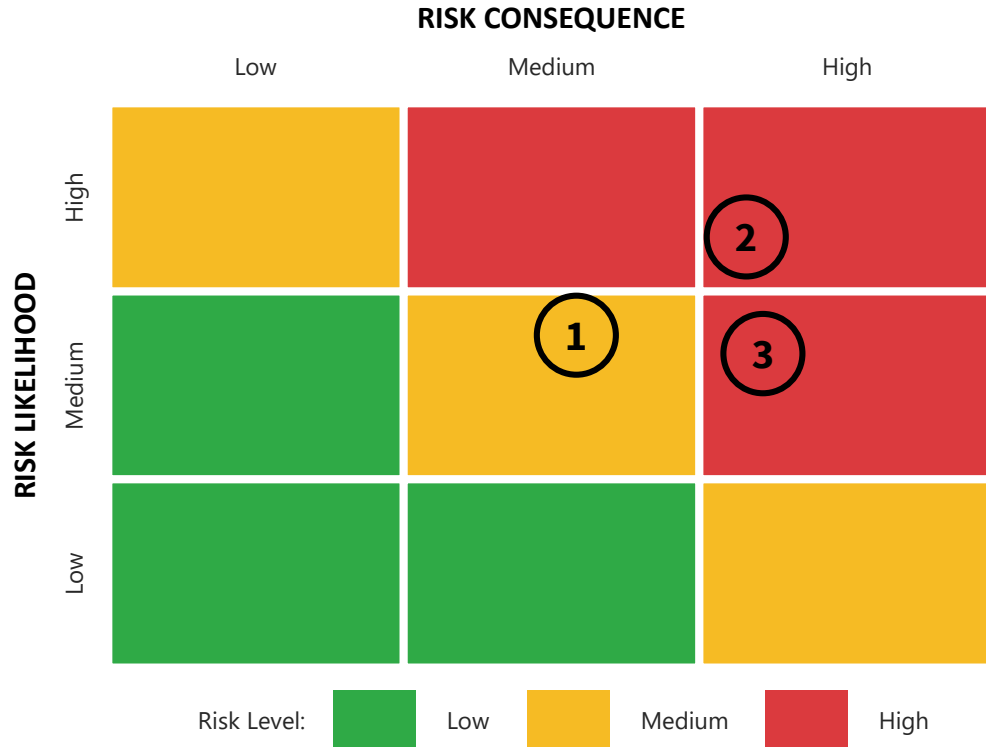
Sicherstellung angemessener Maßnahmen, um die Robustheit zu steigern und im Schadenfall jegliche Fähigkeiten und Services für den Fortbestand des Betriebs wiederherzustellen



# Cyber Risk Assessment

## Risiko Priorisierung

#	RISK DESCRIPTION	RISK MITIGATION PLAN
1	Organisation	Festlegung von Verantwortlichkeiten und Rollen.
2	Mitarbeiter-sensibilisierung	Regelmäßige Durchführung von Mitarbeitersensibilisierungsmaßnahmen.
3	Notfallmanagement	Regelmäßige Durchführung von Notfallübungen mit Cyber-Bezug. Validierung der Wiederanlaufzeiten.



# Cyber Risk Assessment

## Feststellung des Reifegrad







# 5 Öko-System der AXA



“Unsere Kunden erwarten mehr von uns, als nur ihre Rechnungen zu bezahlen. Wir müssen uns auf den Weg machen, ein Partner für unsere Kunden zu werden.”

THOMAS BUBERL  
Chief Executive Officer

# AXA Öko-System

## Payer-to-Partner





# Fazit & Diskussion

# Fazit

... die Frage ist nicht ob, sondern wann

- ➔ Gefahren sind vielfältig und teilweise überraschend
- ➔ Folgen oft nicht ausreichend abschätzbar
- ➔ Schutzmaßnahmen nicht immer (aber oft) möglich
- ➔ Es gibt keine absolute Sicherheit
- ➔ Versicherungsschutz nicht immer möglich – aber öfter, als Sie denken!
- ➔ Bleiben Sie wachsam!



A man in green patterned shorts is diving into the ocean. A large red 'X' is overlaid on the image, with the word 'Danke' written in blue text on the right side of the 'X'.

**Danke**

# Visitenkarte

## **Michael GUIAO**

Cyber Security Consultant  
Kompetenzstelle Cyber  
Industriekundengeschäft  
AXA Konzern AG

Colonia-Allee 10-20  
D-51067 Köln

[michael.guiao@axa.de](mailto:michael.guiao@axa.de)

Tel.: 0221 148-35784

[axa.de](http://axa.de)

