MARSH

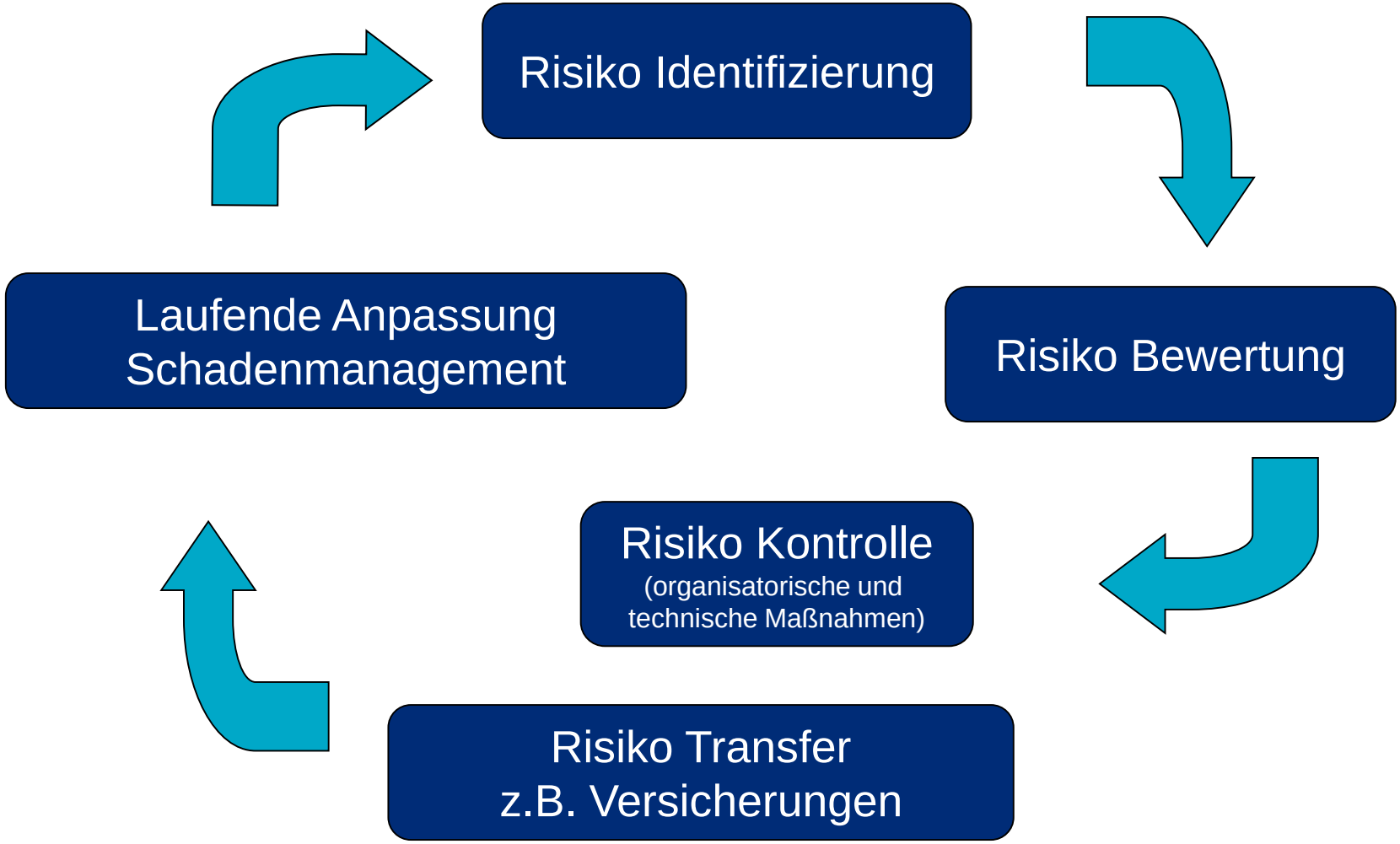
Windenergie, Cyber-Risiken und Datensicherheit

11. November 2015

Dr. Michael Härig
Leiter Branchenteam Power
Marsh GmbH, Düsseldorf

MARSH & McLENNAN COMPANIES

Risiko- und Versicherungsmanagement



Marsh & McLennan Companies
Unternehmensstruktur

Marsh & McLennan Companies
Umsatz: mehr als 12 Mrd. US-Dollar ▪ Niederlassungen in über 100 Ländern ▪ weltweit etwa 54.000 Mitarbeiter

Risiko- und Versicherungsmanagement

Marsh

Versicherungsmakler und Risikoberater

- Weltweit führender Versicherungsmakler und Risikoberater
- Niederlassungen in mehr als 100 Ländern
- 25.000 Mitarbeiter
- In Deutschland ein führender Risiko-berater und Versicherungs-makler
- 8 Büros
- ca. 650 Mitarbeiter

Guy Carpenter

Rückversicherungs-makler

- Weltweit führender Rückversicherungsmakler
- Niederlassungen in über 50 Ländern
- 2.400 Mitarbeiter

Beratung

Mercer

Globaler Anbieter für Consulting, Outsourcing und Investments

- Weltweit führender Berater für Personal-management und damit zusammen-hängende Fragen des Finanz-management
- Niederlassungen in mehr als 40 Ländern
- ca. 19.000 Mitarbeiter

Tochtergesellschaften
- Mercer HR Services
- Mercer Global Investments

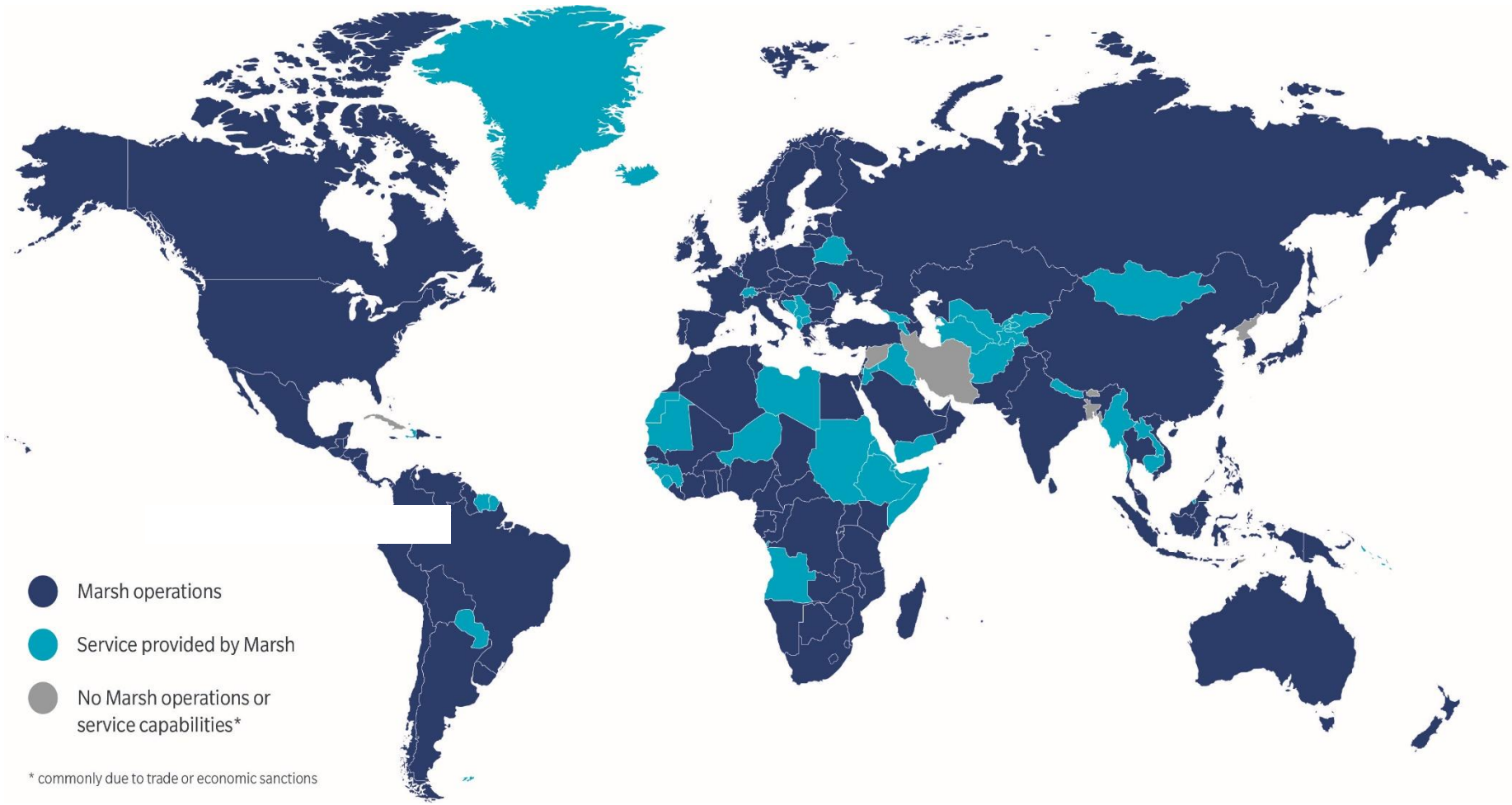
Oliver Wyman

Unternehmensberatung

- Führende, weltweit tätige Unternehmensberatung
- Niederlassungen in 16 Ländern
- ca. 3.400 Mitarbeiter

Tochtergesellschaften
- Lippincott
- Nera Economic Consulting

Wir sind in Ihrer Nähe
Weltweit



MARSH
Unsere Branchenexpertise – Ihr Vorteil

- Gleiche Branche = die wesentlichen Risiken sind gleich

  ⏩ Branchenteam MIP: Marsh Industry Practice

- MIP Power: eins von ca. 20 Branchenteams für die Energiewirtschaft

- Weltweites Netzwerk von Ingenieuren, Naturwissenschaftlern, Juristen, Betriebswirten und Versicherungsexperten mit Branchen-Expertise

- Im deutschen Markt > 22 GW Erneuerbare Energien platziert

→ **Schadenverhandlungen auf Ingenieursniveau**

Optimal angepasste Lösungen für die Energiebranche

Wind (on/offshore), Photovoltaik, Biomasse/-gas, Geothermie, MVA

MARSH

CYBERBEDINGTE RISIKEN

MARSH & McLENNAN COMPANIES

So sehen wir Ihre Risiken
Risikotransfer auf Cyber-Risk-Versicherungen möglich

Angriff-setzung

auf Ziel

durch Einwirkungs-möglichkeiten auf

Jamie Shea, Vize-Generalsekretär Nato für neue Bedrohungen zu Cyber-Attacken und Gegenstrategien (**Quelle: Wiener Zeitung.at am 30.04.2015**)

Frage: Wie häufig sind Cyber-Attacken auf die Nato?

Häufigkeit: ca. **2000 Attacken im Monat**

In Gleichartigkeit zu: größeren Firmen, Organisationen und Ministerien

Unterscheidbar nach: Intention (, z.B. Test oder ausgeklügelte Attacke)

Zitat:

„…Das klingt nach sehr viel, aber es ist nicht besonders ungewöhnlich, jedem Ministerium und jeder größeren Firma oder Organisation geht es gleich. Man muss zudem zwischen leichten Attacken unterscheiden, bei denen nur irgendjemand unser System testen will - und ausgeklügelteren Attacken, bei denen wirklich jemand in unser System einbrechen will. Bei Letzteren ist die Zahl natürlich viel geringer.“

Cyber-Risiken
Konsequenzen

Datenleck
- Bsp.: Datenverlust, Weitergabe persönlicher Daten
- Daten werden von Hackern gestohlen
- Zeit zwischen Angriff und Entdeckung: 230 Tage

Herausforderungen für die IT
- Problem beheben
- Tagesgeschäft weiterführen

Reputation
- Information der Kunden
- Verlust von Kundenvertrauen

Vermögensschaden
- Ursachenforschung
- Wiederherstellung von Sicherheit, Daten und Systemen
- Unterbrechung des Geschäftsbetriebes
- Bußgelder, Schadenersatz

Risiken für die Unternehmensorgane
- Unerwartete Kosten/Umsatzeinbrüche

Bedrohungspotentiale
Beispiele für die Windenergiebranche

Anlagenbetreiber

- Stillstand (Einfluss auf Steuerung, fehlerhafte Sensorik)
- Beschädigung (Manipulation CMS)

  (auch Risiken des Verfügbarkeitsgarantiegebers)

Netzbetreiber

- Ausfall
- Auch Risiko des Energieerzeugers

WEA-Hersteller

- Störung in Lieferkette, Produktionsausfall (Industrie 4.0)
- Mangelhafte Elektronik/Software wirkt sich auf Verfügbarkeit aus

Wartungsfirmen

Fernüberwachung (Abschaltung mehrerer GW)

Direktvermarktung

Einstufung Bedrohungsumfeld 1/2 - Welche Motivationslagen sind erkennbar?

- **Kriminelle Intention**

  Organisierte (Wirtschafts-)Kriminalität:

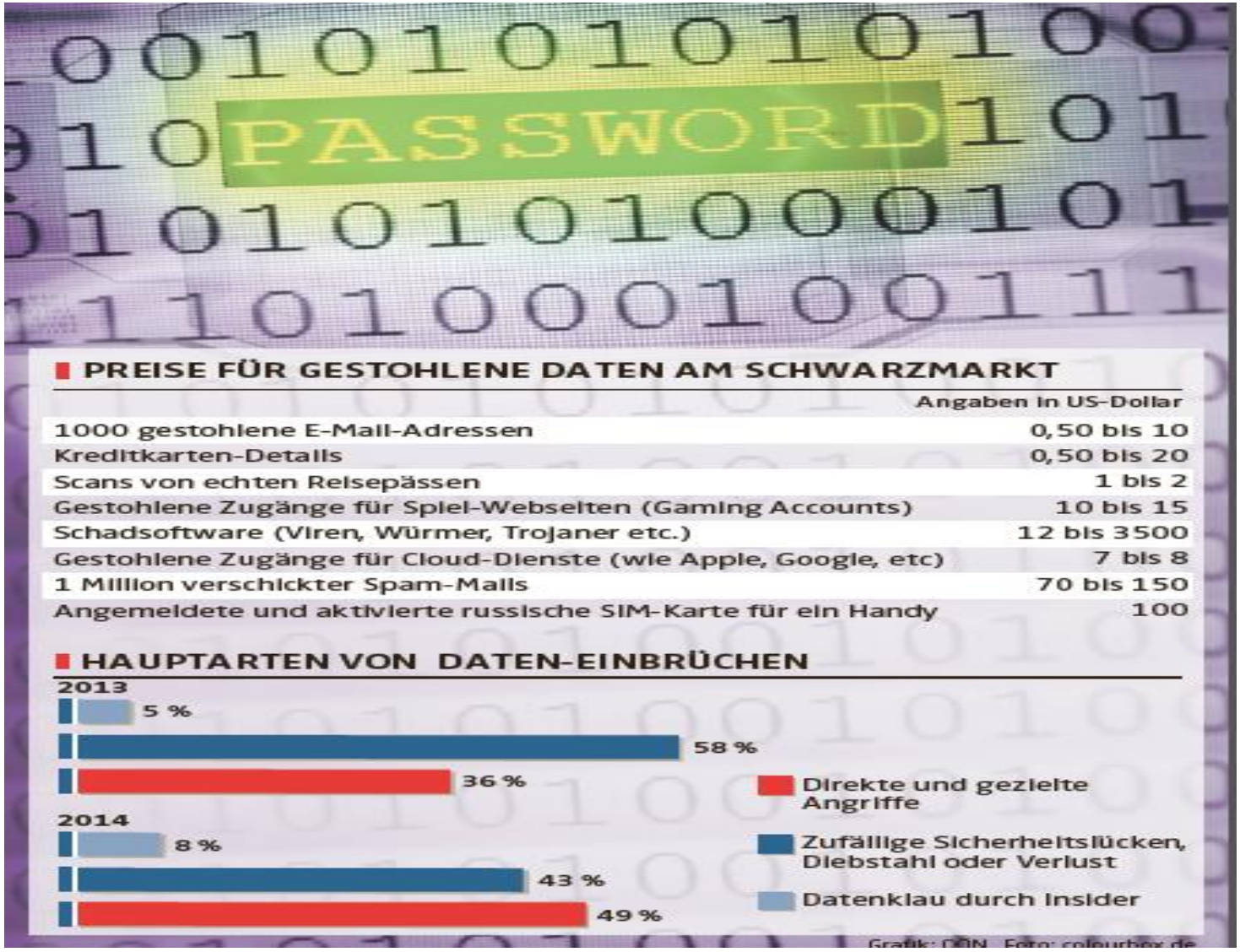
  Hacking hat sich zu einer der Hauptaktivitäten organisierter Wirtschaftskriminalität entwickelt, da ein lukrativer Markt für erlangte Informationen besteht und bedient wird.

  Ziel: Erlangung verwertbarer Daten;

  Wirtschaftsspionage
  (Strategien, Schlüsselpersonal, F&E)

  Digitalisierte Daten einer betrieblichen Organisation sind geldwert, da mindestens an den Berechtigten veräußerbar

Preisliste der durch Kompromittierung gewonnenen Datensätze



Quellennachweis:
Artikel „Das kosten Ihre gehackten Daten auf dem weltweiten Internetschwarzmarkt“ aus nachrichten.at vom 02.05.2015

Einstufung Bedrohungsumfeld 2/2 - Welche weiteren Motivations-lagen sind erkennbar?

- **Terroristisch oder staatlich motiviert gesteuerte Aktivitäten, auch weltanschauungsabhängig**

Die Fähigkeit, mit einer bloß immateriell aus der Ferne führbaren Einflussnahme einen realen physischen Schaden zu erzielen, stellt insbesondere ein für staatlich und ideologisch motivierte Täter attraktives, weil sicheres Umfeld dar.

Ziel: Durch erreichbare Schadenausmaß definiert. Insbesondere Teilnehmer kritischer Infrastrukturen stehen im Fokus.

Wie ist das Bedrohungsumfeld einzustufen? Welche Motivationen sind darüberhinaus erkennbar?

- **„Hacktivisten“**

  Gruppierungen von Hackern bündeln vorhandene Kapazitäten, um unterschiedlich motiviert Ziele wirksam anzugreifen.

  Häufige Motive (alternative Aufzählung):

  1. Erlangung öffentlicher Aufmerksamkeit zur Verfolgung eines Sekundärzieles

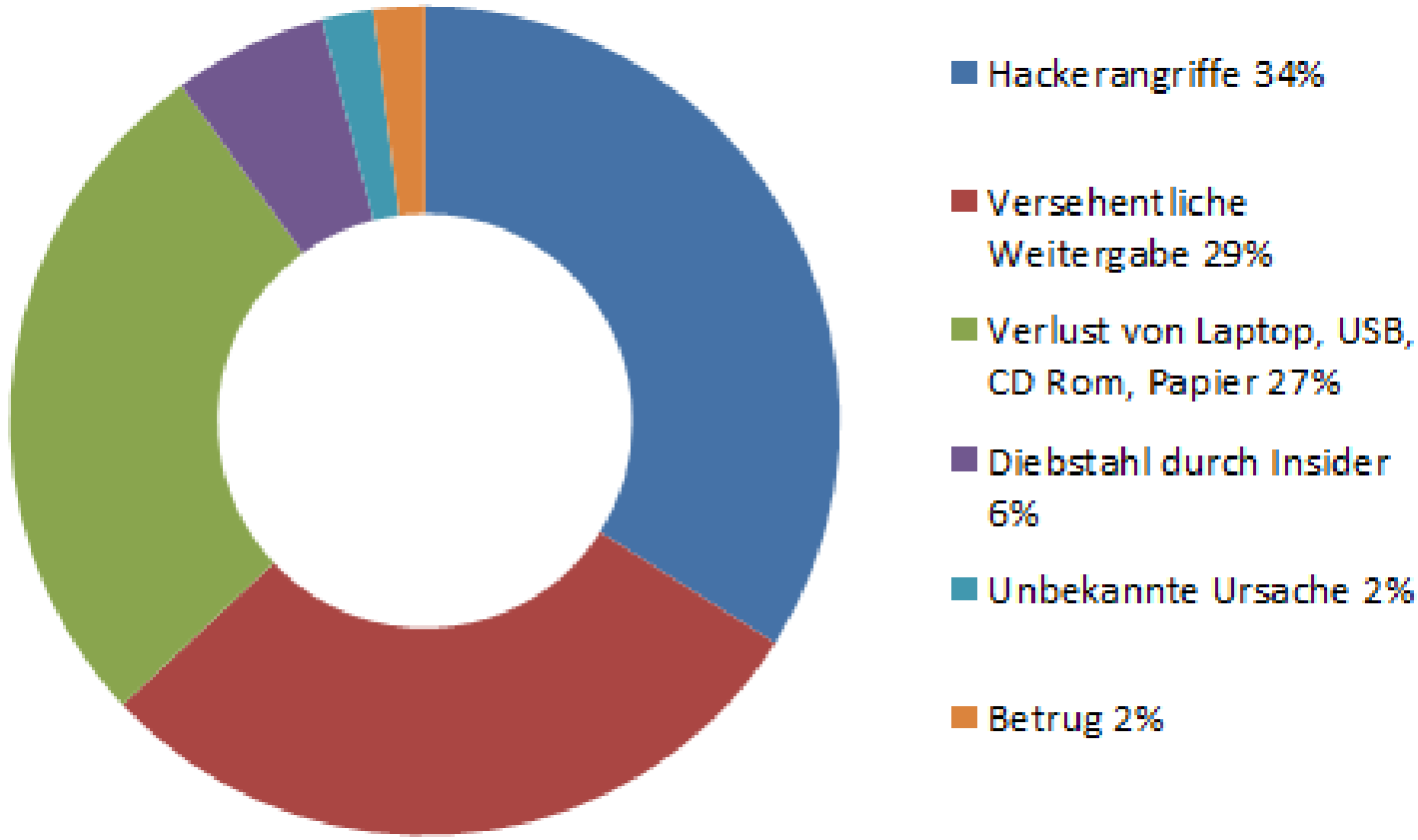
  2. Eine branchenweite, mindestens jedoch unternehmensweite Wirkung zu erzielen (Sekundärziel)

  3. **Wirtschaftliche Motivation** (Entgeltliche Dienstleistung ähnlich werkvertraglicher Art)

Ursachen Sicherheitsvorfälle

62% der Sicherheitsvorfälle haben unternehmensinterne Ursachen

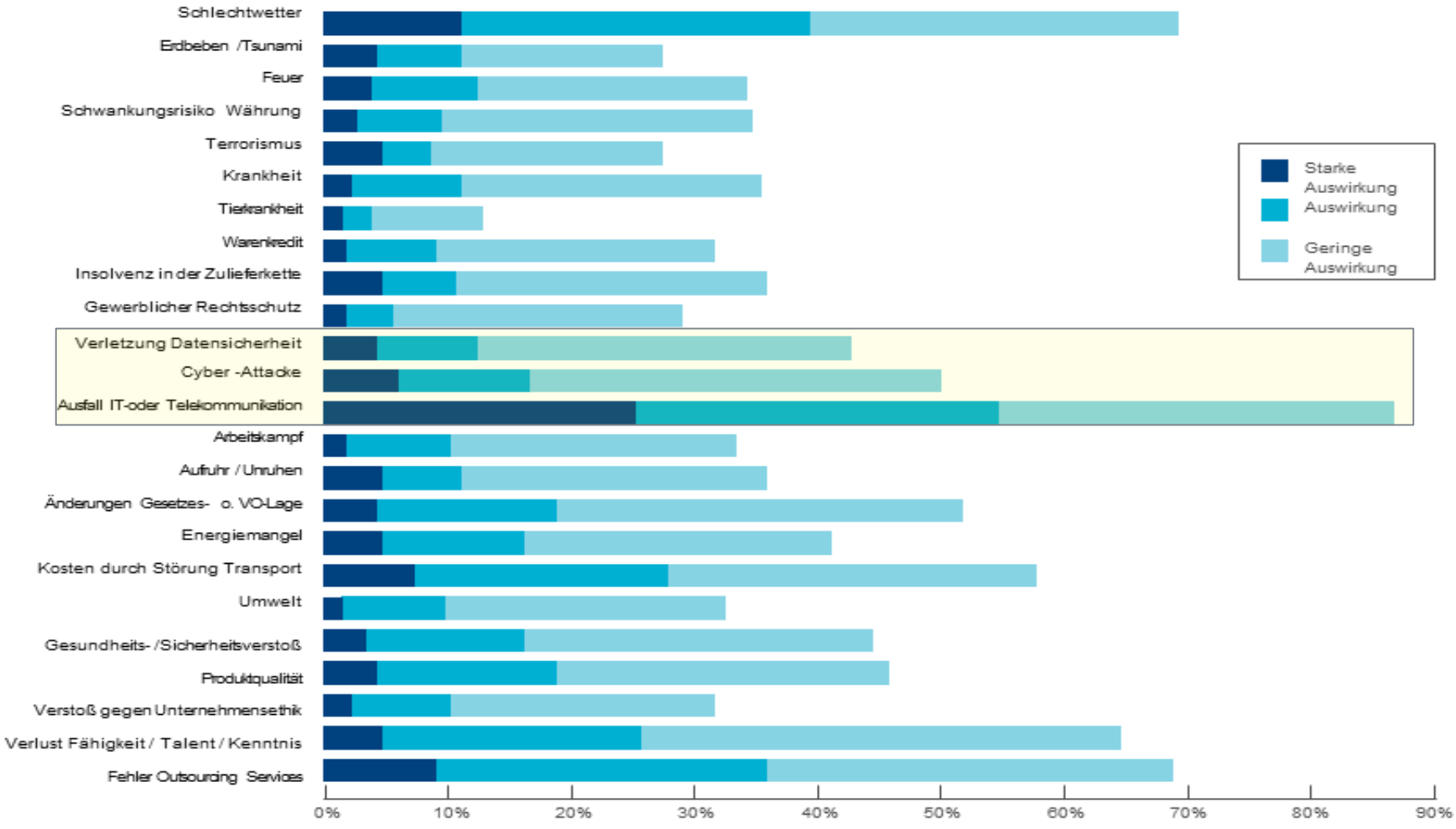
NUR 38% der Sicherheitsvorfälle haben unternehmensexterne Ursachen



Schadenbewertung, branchenübergreifende Betrachtung

Hauptursachen von Störungen in Lieferketten (Quelle: Marsh UK, Stand 2014)

Branchenbezogene Einzelbetrachtung kann einzelne Auswirkungsergebnisse weiter verstärken!



Zahlreiche Schadenbeispiele in der Energiebranche

Datenskandal bei den Stadtwerken Ulm/Neu-Ulm
http://www.swp.de/ulm/lokales/ulm_neu_ulm/SWU-hat-Bankverbindungen-in-unverschluesselten-Mails-verschickt;art1158544,2428146

Ein Hacker brauchte nur zwei Tage, um die Kontrolle über die Stadtwerke in Ettlingen zu übernehmen
http://www.zeit.de/2014/16/blackout-energiehacker-stadtwerk-ettlingen

Heidelberger Stadtwerke bringen Kundendaten durcheinander
http://www.projekt-datenschutz.de/vorfall/heidelberger-stadtwerke-verwechseln-adressen

Augsburger Stadtwerke verschicken irrtümlich Daten von 26.400 Kunden
http://www.augsburger-allgemeine.de/augsburg/Augsburger-Stadtwerke-verschicken-irrtuemlich-Daten-von-26-400-Kunden-id32076747.html

Stadtwerke München: Gehälter der Aufsichtsräte in Massen-E-Mail verschickt
http://www.projekt-datenschutz.de/vorfall/stadtwerke-m%C3%BCnchen-geh%C3%A4lter-der-aufsichtsr%C3%A4te-massen-e-mail-verschickt

Hacker infizieren Schaltzentralen der Stromnetze
http://www.welt.de/wirtschaft/article129674310/Hacker-infizieren-Schaltzentralen-der-Stromnetze.html

Digitale Sorglosigkeit ist für alle Firmen gefährlich
http://www.zeit.de/digital/internet/2015-04/hackerangriff-deutschland-bsi-bericht

Auszug: Anzahl Infrastrukturausfälle außerhalb D

10 August, 2014 **Power outage shuts off traffic lights, affects 3,400 customers around Capitol Hill Seattle**
A power outage shut off traffic lights and residential electricity for an estimated 3,400 customers around Capitol Hill and parts of the Central District Saturday afternoon.

8 July, 2014 **Arizona utility agrees to $3.25M settlement in 2011 blackout that left millions without power**
SAN DIEGO — Federal regulators said Monday that they've approved a $3.25 million settlement with an Arizona utility over a 2011 blackout that left millions of people without power in California, Arizona and Mexico.

8 July, 2014 **Major delays after Channel Tunnel power failure**
Nearly 400 passengers had to be evacuated from the Channel Tunnel on Monday after a power failure caused their train to stop mid-tunnel, sparking major delays and cancellations on the car service and the Eurostar.

29 June, 2014 **Jetstar Seeks Damages From Sydney Airport After Last Week's Blackout**
The T2 terminal at Sydney Airport was brought to a standstill on Friday just after 8.30am, with the power outage causing delays for passengers at check-in and screening.

26 June, 2014 **Power outage hits hundreds in Greenville County, South Carolina**
Duke Energy reported almost 2,000 outages in and area between Mauldin and Simpsonville early Wednesday morning.

27 May, 2014 **50,000 customers without power for an hour in Tucson**
A power outage affecting a large portion of Tucson left 50,000 customers without power for over an hour on Monday.

Infrastrukturausfall **2**

27 May, 2014 **Power outage in West End Sault Ste. Maria, Ontario, Canada**
Power in the West End was restored yesterday after a brief outage around noon affectted 4315 customers.

26 May, 2014 **Power outage affects over 1000 businesses and residents in High Wycombe, England**
A POWER cut disrupted over 1000 businesses and residents in and around High Wycombe this morning.

26 May, 2014 **Power outage causes problems at Rhinelander, Wisconsin Paper Mill**
The paper mill in Rhinelander, Wisconsin wants to get back on track after a partial power outage caused some problems earlier Sunday.

26 May, 2014 **Power outage leaves West Yellowstone in the dark**
Fall River Rural Electric Cooperative customers in and around the areas of Island Park, Idaho, or West Yellowstone experienced interruptions in service Sunday because of a damaged transmission line.

26 May, 2014 **Sunday night left 2,379 customers without power in Sioux City, Iowa**
Mid American Energy is addressing a power outage in Sioux City Sunday night that has left 2,379 customers without power.

25 May, 2014 **A power outage led to major problems at a water treatment plant in North Carolina on Saturday**
A power outage led to major problems at a water treatment plant in King on Saturday.
City officials said a pump failure caused water to enter the plant and shorted an electrical system.

MARSH

Grundlagen der klassischen Versicherungen

Sachversicherungen, Haftpflichtversicherung

MARSH & McLENNAN COMPANIES

Grundlagen der klassischen Versicherungen
Sachversicherung – Schutz eigener Sachen

Sachschaden-Definition:

- Substanzveränderung

und dadurch

- reduzierter
  Wert oder Brauchbarkeit

Grundlagen der klassischen Versicherungen
Sachversicherung – Schutz eigener Sachen

Sachversicherung (Feuer, Maschinen, Elektronik, Montage) inkl. Betriebsunterbrechung

- Sachschäden an eigenen Sachen (Gebäuden, Maschinen, Einrichtungen)
- Entschädigung in der Regel unabhängig von einer Verschuldensfrage
- Versicherte Gefahren:
  Feuer, Maschinenbruch, Unwetter, Diebstahl, Bedienungsfehler,…
  Sachschäden durch Cyber ?
- Betriebsunterbrechungsversicherung:
  Vermögensschaden als Folge eines versicherten Sachschadens
  - Versichert, wenn bei der versicherten Sache ein Sachschaden vorliegt
  - *Rückwirkungsschaden* bei Ausfall einer nicht versicherten Sachen
    z.B. Trafo des Netzbetreibers.
    Aber: am Trafo muss ein dem Grunde nach versicherter Sachschaden vorliegen

Herausforderungen Cyber
Lange Zeit daher nur unzureichend versicherbar

Warum entschädigt die Sachversicherung in vielen Fällen nicht?

- Daten fehlt strenge rechtliche Sacheigenschaft
- Ohne versicherten Sachschaden keine Entschädigung für den Ertragsausfall durch Stillstand.
- Cyber in einigen Bedingungswerken als versicherte Gefahr ausgeschlossen. Damit ist ein aus Cyber resultierender Sachschaden nicht versichert.
- Ohne versicherten Sachschaden ist der Betriebsunterbrechungsschaden nicht versichert.

- Datenverlust als Folge eines Sachschadens des Datenträgers wiederum versicherbar

Grundlegende klassische Versicherungsarten
Schäden Dritter

Haftpflichtversicherung

- Entschädigung für Personen- oder Sachschäden Dritter, die sich aus gesetzlichen Ansprüchen privatrechtlichen Inhalts ergeben.
- In der Regel muss Verschulden nachgewiesen werden (Rechtsschutzfunktion)
- Vermögensschaden gedeckt als Folge eines Personen- oder Sachschadens

- Reine Vermögensschäden nur begrenzt versicherbar
- Ausschlüsse/Limitierungen für Tätigkeits-/Bearbeitungsschäden und Vertragserfüllung

Herausforderungen Cyber
Lange Zeit daher nur unzureichend versicherbar

Warum entschädigt die Haftpflichtversicherung in vielen Fällen nicht?

- Verschuldensnachweis schwierig
- Stillstand eines Rechenzentrums und Verlust von Daten
  - Reiner Vermögensschaden nur eingeschränkt versicherbar
- Nichtbearbeiten von Daten (z.B. Rechnungsabwicklung)
  - Reiner Vermögensschaden Dritter
  - Bearbeitung der Daten ist Vertragserfüllung

Auszug möglicher Highlights eines Deckungsschutzes

Versicherte Kostenpositionen, ausgelöst durch verwirklichte Cyber-Risiken

Kostendeckung, Eigenschadenbereich

- Betriebsunterbrechungskosten, d.h. fortlaufende Kosten und entgangener Gewinn, insbesondere durch
  - Hacker-Attacken
  - Schadprogramme, Viren
  - Hard- und Softwareschäden
-
  - Krisenmanagement
  - PR-Management, unabhängig von Einstufung Sach- oder Personenschaden
- Wiederherstellung von verlorenen Daten und IT-Systemen
- Kosten/Entschädigungszahlung bei Cyber-Erpressung
- Entstandene Mehrkosten IT-Ausfall oder Missbrauch Telefonanlage

Ansprüche von außen, Drittschadenbereich

- Vermögensschäden, insbesondere durch
  - Persönlichkeitsrechtsverletzungen, auch eigener Mitarbeiter
  - Urheberrechtsverletzungen
  - Verletzung des Bundesdatenschutzgesetzes
  - Verlust der Vertraulichkeit von Daten
  - Produktfehler / Fehler bei der Erbringung von Leistungen
  - Übertragung von Viren
  - Verzug der Leistung
  - Schadenersatz wegen Nichterfüllung
  - Austausch von Kreditkarten
- Vertragsstrafen / Bußgelder (PCI)

Kritik an klassischen Versicherungen
Deckungslücken und (evtl. teilweise existente) Doppelversicherungsmöglichkeiten

Risiken im Umgang mit Daten	**In der Regel angebotener Versicherungsschutz**					**Cyber-Risk-Versicherung**
	Sach-Versicherung	**Betriebsunterbrechungs-Versicherung**	**Betriebshaftpflicht-Versicherung**	**Vertrauensschaden-versicherung**	**Managerhaftpflicht-Versicherung (D&O)**	
Deckungsauslösendes Moment:	Versicherter **Sachschaden**	Versicherter **Sachschaden**	eigenes **Verschulden**	Kriminelle Handlung (**Bereicherungsabsicht**)	Pflichtverletzung	Verlust von Daten oder IT-Störung
Deckung bereits im Verdachtsfall						✓
Hackerangriff / Datenkompromittierung				✓		✓
Betriebsunterbrechung nach Hackerangriff oder Denial of Service Attacke						✓
Diebstahl von Daten				✓		✓
Wiederherstellung von Daten, Software, Netzwerken, etc.				✓		✓
Verlust von Daten durch blosses Liegenlassen					✓	✓
Kosten durch den Verlust von Daten	✓	✓			✓	✓
mittelbare und unmittelbare Vermögensschäden					✓	✓
Haftung für Vertragsvereinbarungen mit Kreditkartenunternehmen (PCI)						✓
Persönlichkeitsrechtsverletzung						✓
Übernahme der Kosten bei einem Datenschutzvorfall						✓
Zugriff auf externe Sicherheitsexperten						✓
Rechtsbeistand			✓		✓	✓
PR / Krisenmanagement					✓	✓
Zahlung von Erpressungsgeldern						✓

Legende: versichert ✓ | nicht versichert

Schadenbeispiel (Versicherungsfall)
Stillstand in der Produktion

Schadenszenario

Böswillige Löschung der Entwicklungsdaten und Produktionsparameter einer gesamten Produktreihe

Schadenbild

- Durch Personalabbaumaßnahmen wird ein Mitarbeiter der IT-Abteilung entlassen
- Dieser ist über seine Entlassung so verärgert, dass er Rache an dem Unternehmen übt
- Er besitzt Kenntnisse darüber, auf welchen Festplatten sich die sensiblen Produktinformationen einer aktuellen Produktion befinden und löscht diese. Darüber hinaus werden die entsprechenden Backupbänder unbrauchbar gemacht
- Die Produktion steht 4 Tage still

Finanzielle Auswirkungen

Datenrettung aus verbliebenen Datenfragmente auf den Festplatten	145.000 €
Forensische Untersuchungen	60.000 €
Produktionsausfall für 4 Tage	940.000 €
Vertragsstrafen an B2B Kunden	500.000 €
Aufspielen von Back-up-Daten	40.000 €
Kosten für Krisenmanager und Rechtsanwalt	90.000 €
Versicherte Gesamtkosten	**1.775.000 €**

Quelle: ACE Versicherung, 2013

Schadenbeispiel (Versicherungsfall)
Hacker sorgt für Stromausfall im Stadtwerk

Schadenszenario

Ein Hacker dringt in das System der Stadtwerke ein und verursacht einen Stromausfall, der 46 Stunden andauert.

Schadenbild

- Die Stadtwerke werden Opfer mehrerer gezielter Hackerattacken
- Durch das Ausnutzen einer Sicherheitslücke dringt ein Hacker schließlich unbemerkt in die Systeme der Stadtwerke ein
- Systemdaten werden so modifiziert, dass es zu einer schweren Störung in der Steuerungstechnik kommt und in Folge dessen das Kraftwerk still steht
- Es kommt zu einem Ausfall der Stromversorgung
- Die vollständige Behebung der Störung dauert 46 Stunden an

Finanzielle Auswirkungen	
Umsatzeinbußen durch Stromausfall	2.300.000 €
Forensische Untersuchungen	40.000 €
Vertragsstrafen	1.500.000 €
Sachverständigenkosten	30.000 €
Versicherte Gesamtkosten	**3.870.000 €**

Quelle: ACE Versicherung, 2013

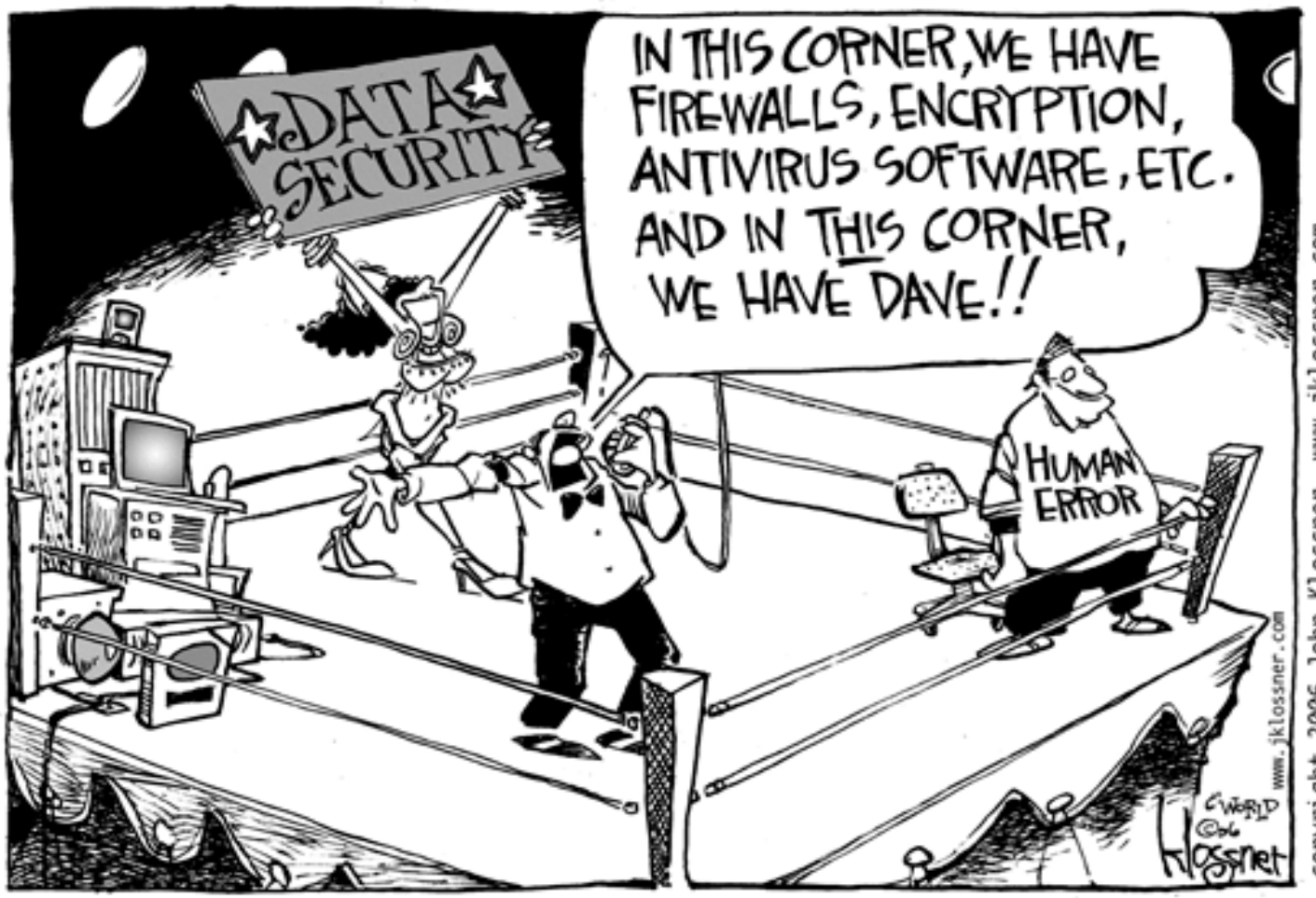
Unsere IT-Systeme sind sicher und immer auf dem neuesten Stand.

In 50% aller Datenschutzvorfälle sind unachtsame Mitarbeiter der Grund für Datenschutzvorfälle.

Hierbei sind vor allem verlorene Laptops, Smartphones, USB-Sticks oder einfach Papier-Akten betroffen.

Kann Ihre IT-Abteilung datenbezogene Krisen professionell managen, **ohne Beweisvernichtung** zu betreiben?

Die traurige Wahrheit



MARSH

Allianz für Cyber-Sicherheit
Partner

“The problem is not insurance, it is risk….”

Henry Marsh 1901

Dr. Michael Härig
Leiter Branchenteam Power

Marsh GmbH
Kasernenstr. 69, 40213 Düsseldorf

+49 (0)211- 8987 368
michael.haerig@marsh.com

MARSH & McLENNAN COMPANIES