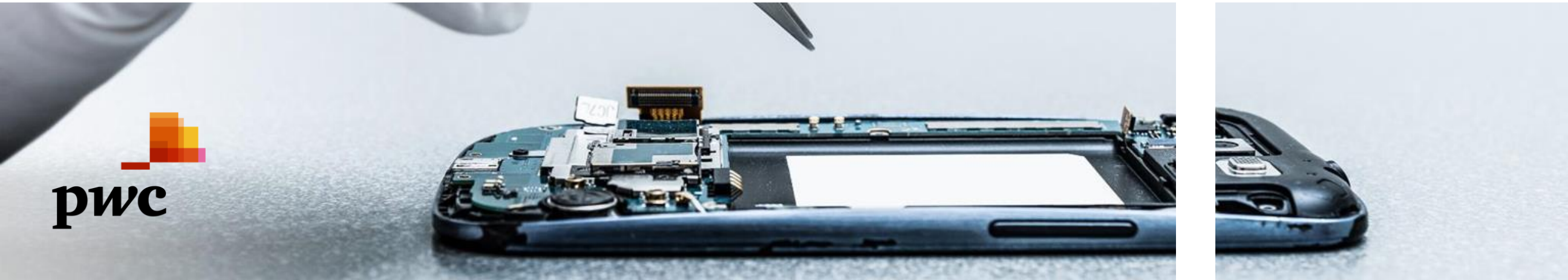
BETRIEBSSPIONAGE FÜR 45 DOLLAR

Juni 2019

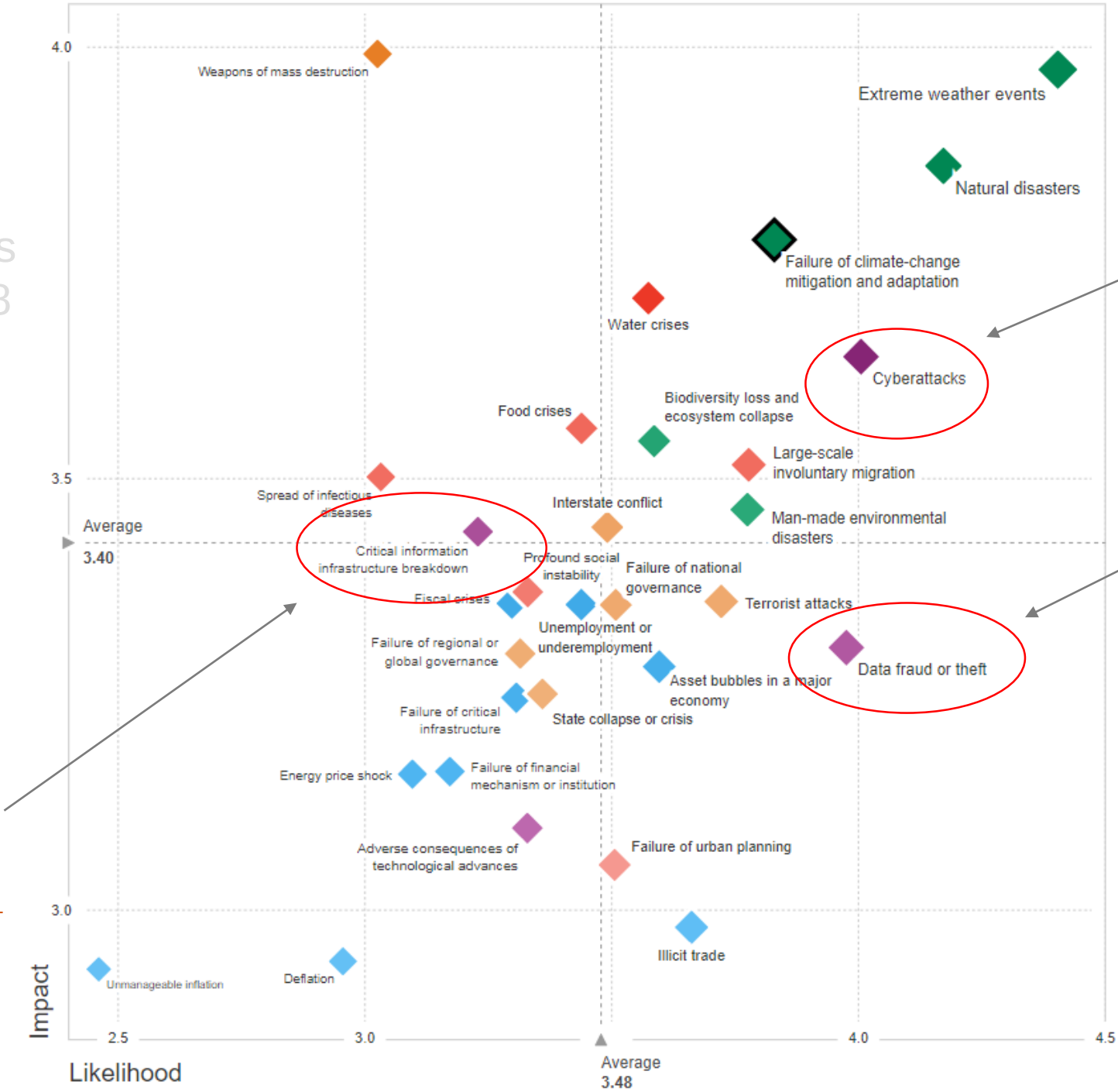


pwc

01

Zahlen & Fakten

The Global Risks Landscape 2018

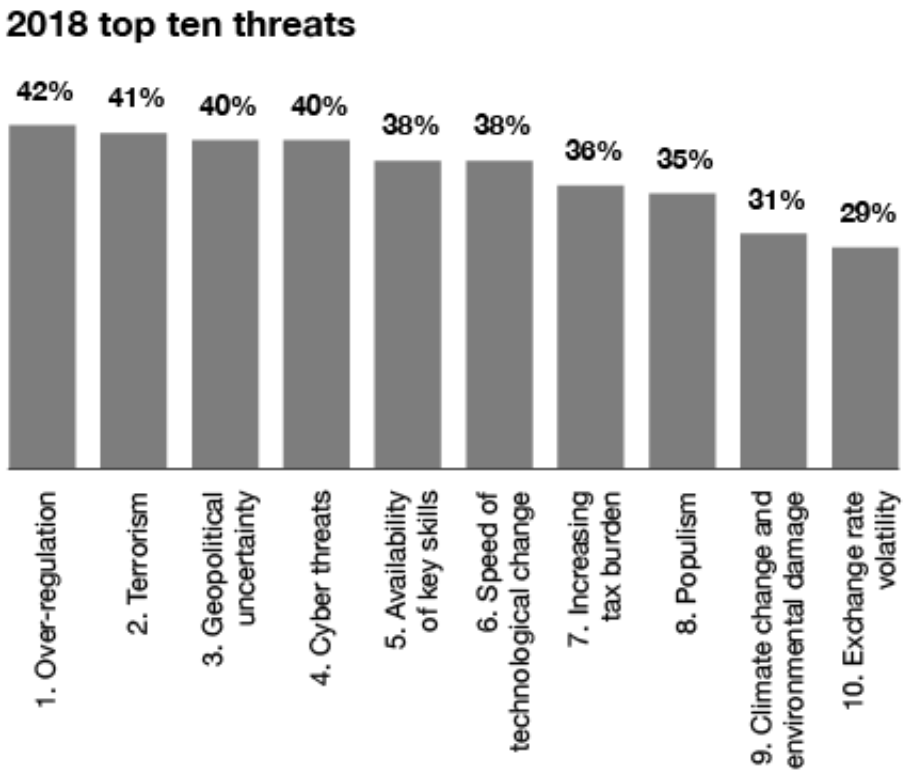


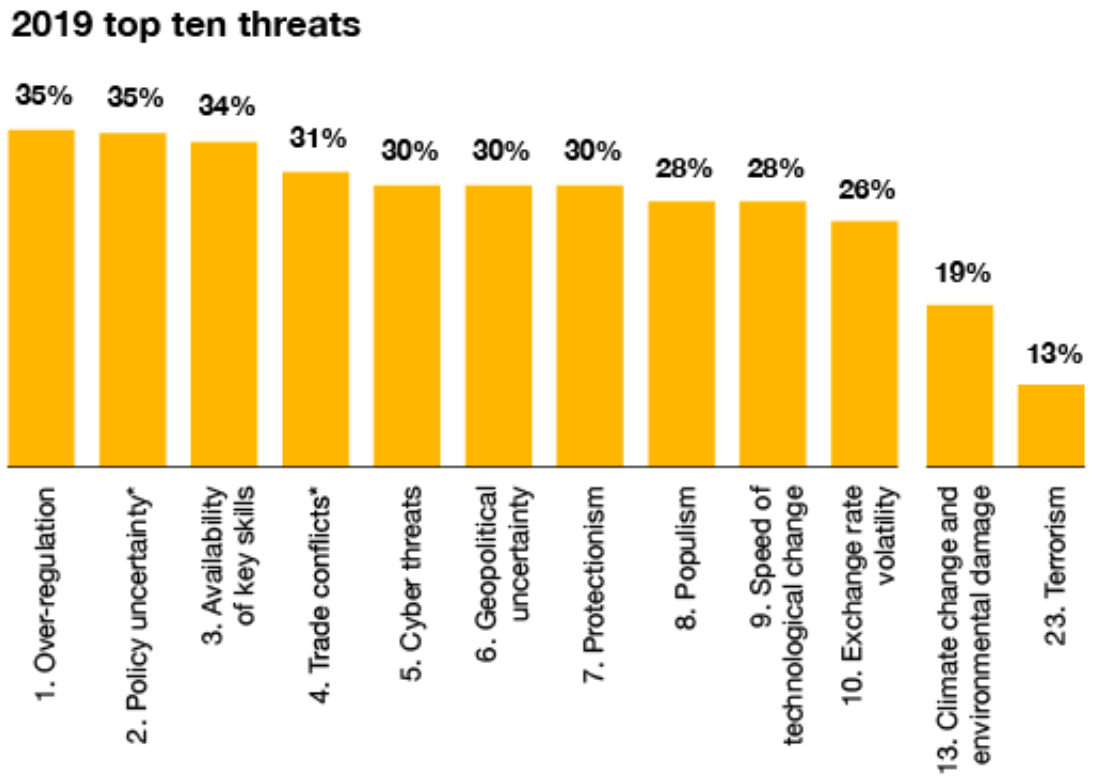
Cyberattack

Data fraud or theft

Critical Information infrastructure breakdown

Cyber threats keep CEOs up at night
PwC's CEO Survey at World Economic Forum in Davos





Ransomware

Bekannte und verbreitete Bedrohungen

Once upon a time at the train station…

02

Betriebsspionage für $45

Betriebsspionage für $45

Mitarbeiter

- ***Ein Mitarbeiter nutzt sowohl am Arbeitsplatz als auch mobil sein Notebook.***
- ***Daten oder Informationen werden zwischen den Kollegen u.a. auch per USB-Stick ausgetauscht.***
- ***Daten/Informationen werden auch mit Kunden per USB-Stick ausgetauscht.***

Mitarbeiter

01

Betriebsspionage für $45

Mitarbeiter

- ***USB Stick mit Unternehmenslogo wird am Parkplatz gefunden.***
- ***Notebooks sind mit Anti-Malware, Firewall, usw. geschützt.***
- ***USB Stick wird durch den Mitarbeiter geprüft und an das Notebook angesteckt.***

02

… findet USB-Stick …

Betriebsspionage für $45

Mitarbeiter

… findet USB-Stick

Rubber Ducky

03

… Angreifer hat Zugriff auf Mitarbeiter Notebook…

- *Keylogger/Reverse-Shell wird gestartet*
- *Zugriff auf alle Dateien des IT-Systems*
- *Video/Audio Daten werden aufgezeichnet*

Betriebsspionage für $45

Mitarbeiter

… findet USB-Stick

Rubber Ducky

… Angreifer hat Zugriff auf Mitarbeiter-Laptop

04

… Zugangsdaten werden gestohlen…

- ***Aufruf der Tesla-Webseite und Anmeldung mittels Eingabe der Zugangsdaten***
- ***Diebstahl der Zugangsdaten***

Betriebsspionage für $45

Mitarbeiter

… findet USB-Stick

Rubber Ducky

… Angreifer hat Zugriff auf Mitarbeiter-Laptop

… Zugangsdaten werden gestohlen

05

… Angreifer hat Zugriff auf Mitarbeiter Notebook…

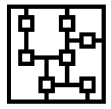
- *Keylogger/Reverse-Shell wird gestartet*
- *Zugriff auf alle Dateien des IT-Systems*
- *Video/Audio Daten werden aufgezeichnet*

03

Wie kann man sich schützen?

Wie kann man sich schützen?

Vorsicht bei der Verwendung fremder USB Sticks



Einsatz von 2-Faktor-Authentifizierung

Durchführen von Mitarbeiter Awareness-Schulungen

Einsatz von Schutzmaßnahmen wie Sichtschutzfolien, Webcam-Abdeckung

Einsatz von Password-Safes zur sicheren Verwaltung von Passwörter

Meldung an die IT-Abteilung im Notfall

Sensibilisierung & Training

Game of Threats – Cyber Arena – Spear Phishing

Game of Threats

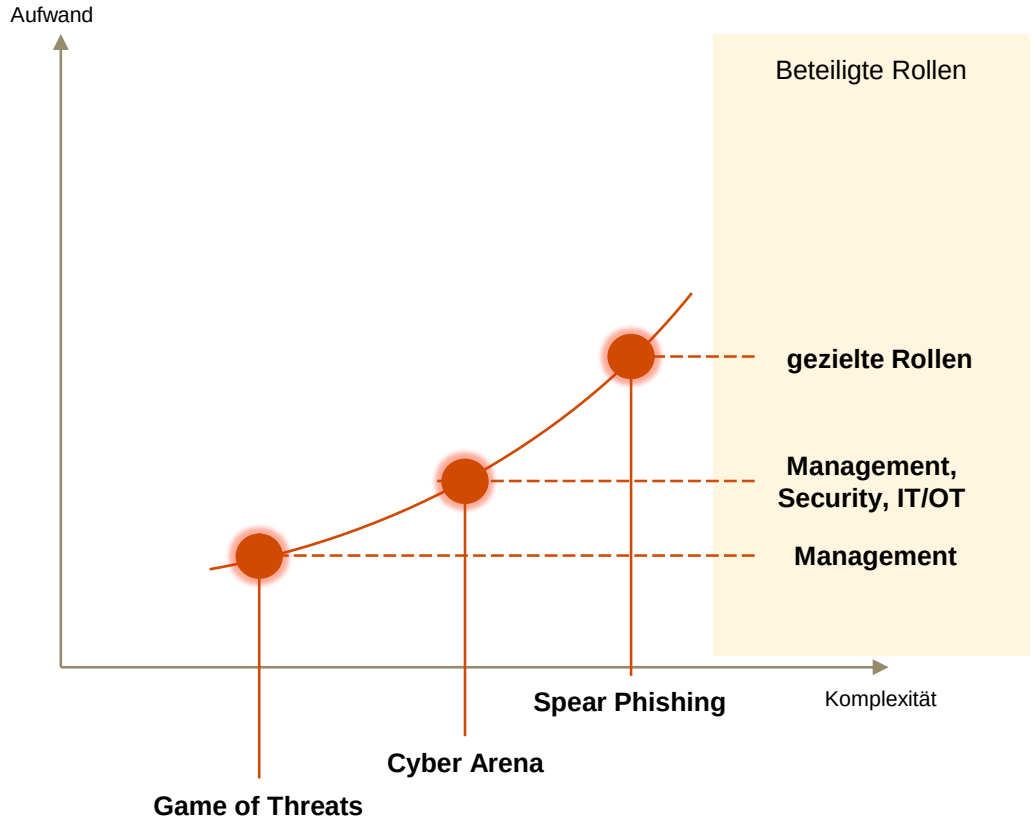
Versetzen Sie sich in die **Rolle des Unternehmens** sowie des **Angreifers**. Unserer interaktive **Cyberangriffssimulation** für das Management.

Cyber Arena

Stellen Sie als Management, Security & IT sowie OT Ihre „**Cybersecurity-Readiness**“ auf die Probe und verteidigen Sie Ihre Werte gegen einen Cyberangriff.

Spear Phishing

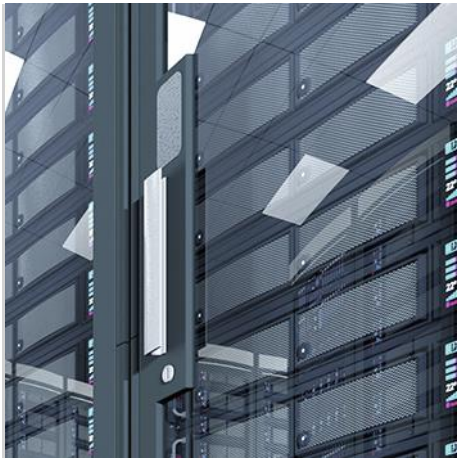
Mit Hilfe gezielter Fake E-Mails simulieren wir einen gezielten **Phishing-Angriff** um die **Erkennungsrate** und den **Sensibilisierungsgrad** Ihrer Mitarbeiter zu messen.



PwC Cybersecurity & Privacy

Informations-sicherheit & Datenschutz

Technical Security



Business Continuity & Krisenmanagement

Managed Security Services

Thank you

Georg Beham
Partner
Cybersecurity & Privacy
Tel. +43 732 611 750 19
georg.beham@pwc.com

Markus Sojer
Manager
Cybersecurity & Privacy
Mobil +43 676 83377 9824
markus.sojer@pwc.com

pwc.at