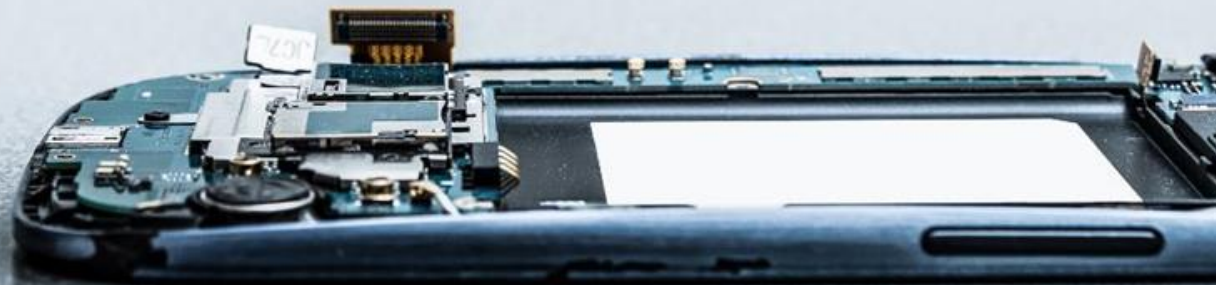


# BETRIEBSSPIONAGE FÜR 45 DOLLAR

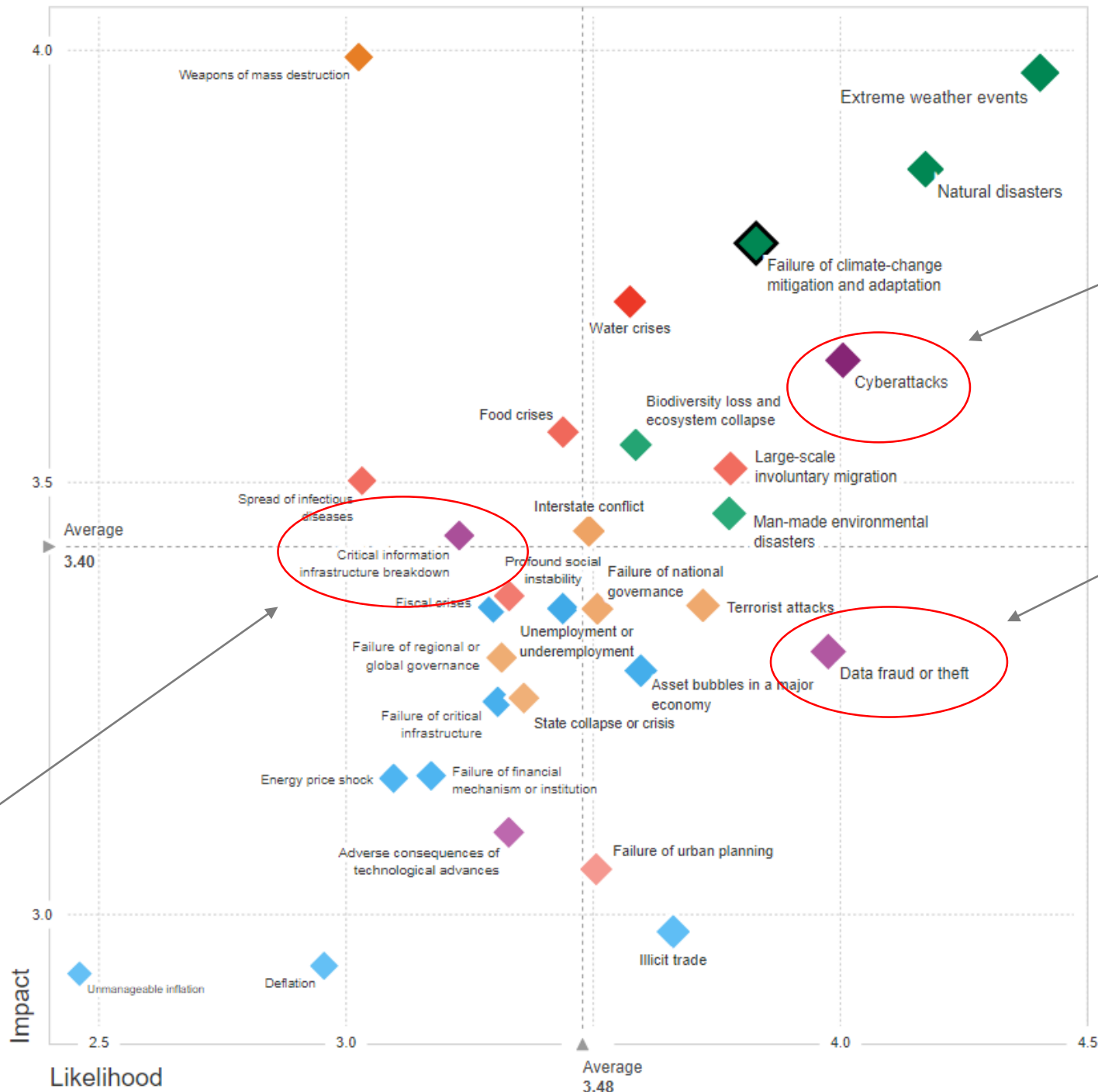
Juni 2019



# 01

## Zahlen & Fakten

The Global Risks Landscape 2018



Cyberattack

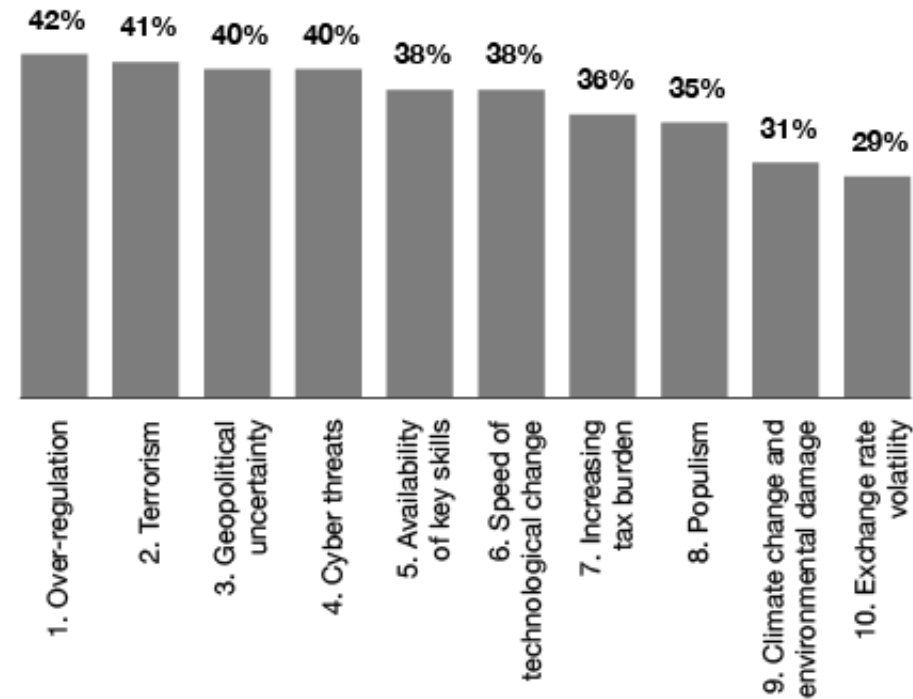
Data fraud or theft

Critical Information infrastructure breakdown

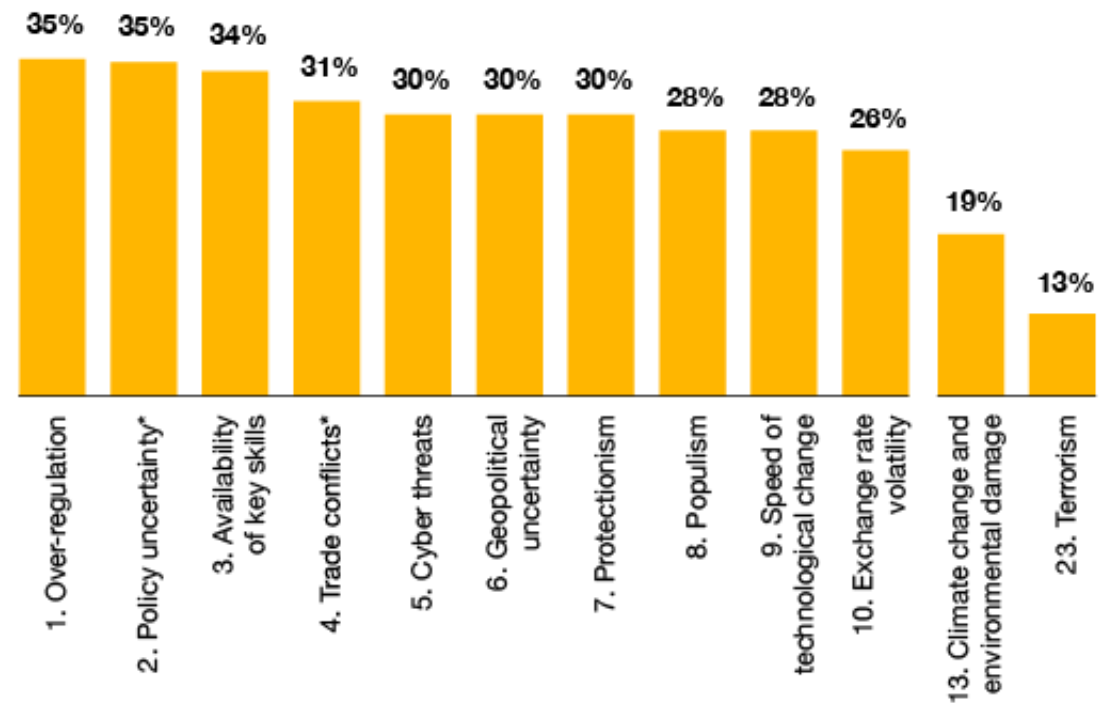
# Cyber threats keep CEOs up at night

## PwC's CEO Survey at World Economic Forum in Davos

2018 top ten threats



2019 top ten threats



# Ransomware

## Bekannte und verbreitete Bedrohungen



**Ooops, your files have been encrypted!** English

**What Happened to My Computer?**  
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

**Can I Recover My Files?**  
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

**How Do I Pay?**  
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

**Payment will be raised on**  
5/16/2017 00:47:55  
Time Left  
02:23:57:37

**Your files will be lost on**  
5/20/2017 00:47:55  
Time Left  
06:23:57:37

[About bitcoin](#)  
[How to buy bitcoins?](#)  
**Contact Us**

**Send \$300 worth of bitcoin to this address:**  
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

bitcoin ACCEPTED HERE

Once upon a time at the  
train station...

Abfahrt	Linie	Ziel	Gleis
22:10	Floha - Pockau-Lengefeld	Nach	8
22:30	Floha - Freiberg	Olbernhau	11
22:30	Floha - Freiberg	Hbf	10
22:31	Floha - Freiberg	(S) Hbf	8
22:36	Floha - Zschopau	g-B. Süd	9
22:36	Floha - Freiberg	Hbf	5
22:44	Geithain - Borsdorf	Hbf	14
22:45	Einsiedel - Thalheim (Erzgeb)	Aue (Sachs)	11
23:30	Floha - Freiberg (Sachs) - Tharandt	Dresden Hbf	

BMG | MIS





# 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

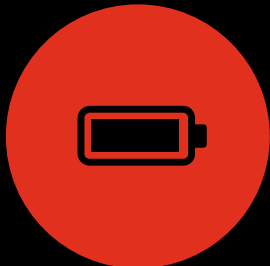
*... findet USB-Stick ...*



# Betriebsspionage für \$45



*Mitarbeiter*



*...findet USB-Stick*



*Rubber Ducky*

03

*... Angreifer hat  
Zugriff auf Mitarbeiter  
Notebook...*

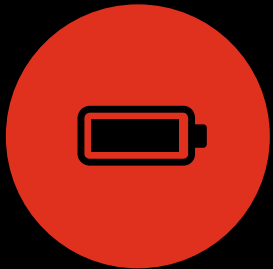
- *Keylogger/Reverse-Shell wird gestartet*
- *Zugriff auf alle Dateien des IT-Systems*
- *Video/Audio Daten werden aufgezeichnet*



# Betriebsspionage für \$45



*Mitarbeiter*



*...findet USB-Stick*



*... Angreifer hat  
Zugriff auf  
Mitarbeiter-Laptop*



*Rubber Ducky*

04

*... Zugangsdaten  
werden gestohlen...*

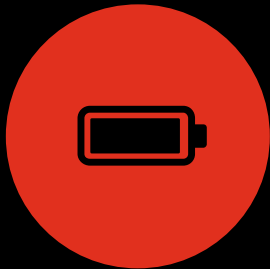
- *Aufruf der Tesla-Webseite und Anmeldung mittels Eingabe der Zugangsdaten*
- *Diebstahl der Zugangsdaten*



# Betriebsspionage für \$45



*Mitarbeiter*



*...findet USB-Stick*



*... Angreifer hat Zugriff auf Mitarbeiter-Laptop*



*... Zugangsdaten werden gestohlen*



*Rubber Ducky*

05

*... Angreifer hat Zugriff auf Mitarbeiter Notebook...*

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



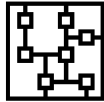
# 03

**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.



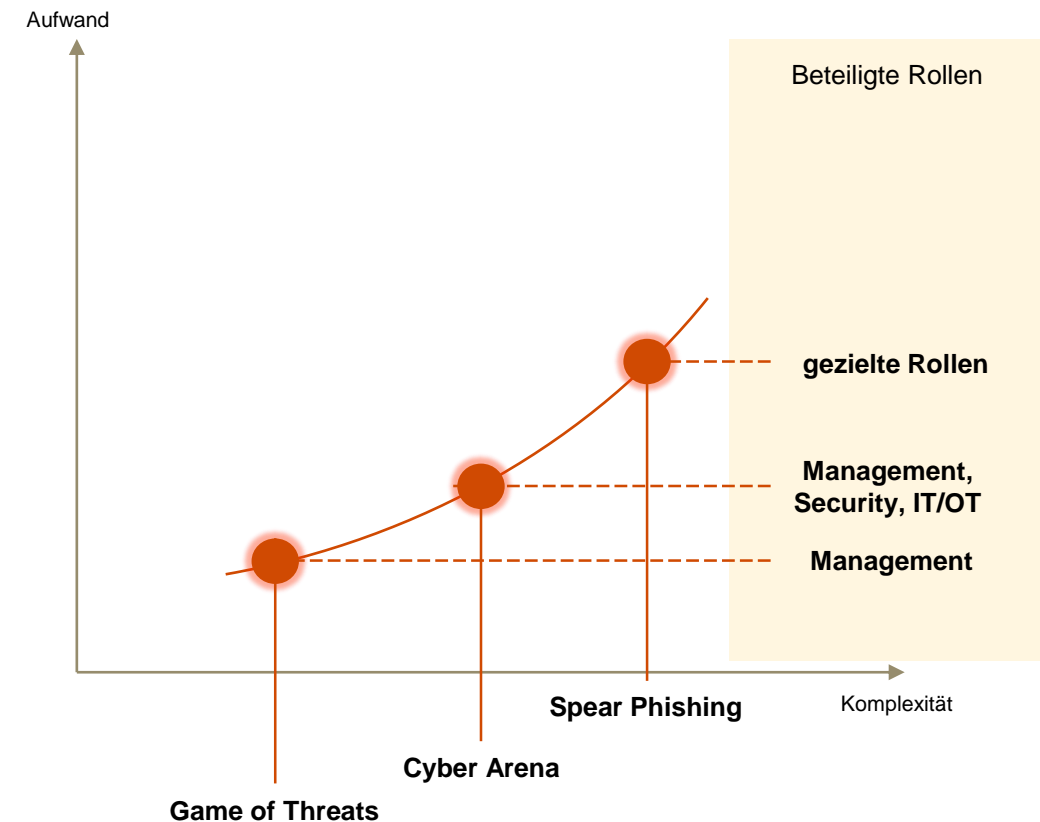
### Cyber Arena

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



### Spear Phishing

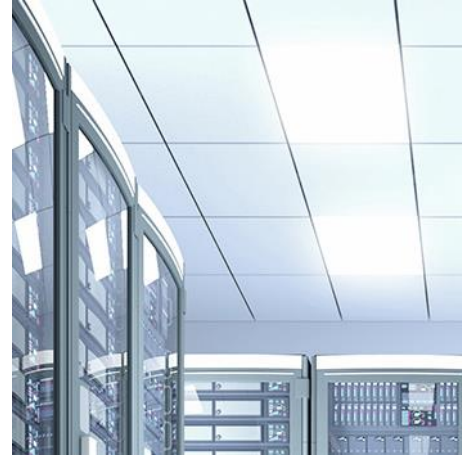
Mit Hilfe gezielter Fake E-Mails simulieren wir einen gezielten **Phishing-Angriff** um die **Erkennungsrate** und den **Sensibilisierungsgrad** Ihrer Mitarbeiter zu messen.



# PwC Cybersecurity & Privacy



**Informationssicherheit & 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](mailto:georg.beham@pwc.com)



***Markus Sojer***

Manager

Cybersecurity & Privacy

Mobil +43 676 83377 9824

[markus.sojer@pwc.com](mailto:markus.sojer@pwc.com)

[pwc.at](http://pwc.at)

© 2019 PwC Österreich. „PwC“ bezeichnet das PwC-Netzwerk und/oder eine oder mehrere seiner Mitgliedsfirmen. Jedes Mitglied dieses Netzwerks ist ein selbstständiges Rechtssubjekt. Weitere Informationen finden Sie unter [pwc.com/structure](http://pwc.com/structure).