Warth & Klein Grant Thornton

An instinct for growth™

Governance, Risk & Compliance

Cyber Security Services

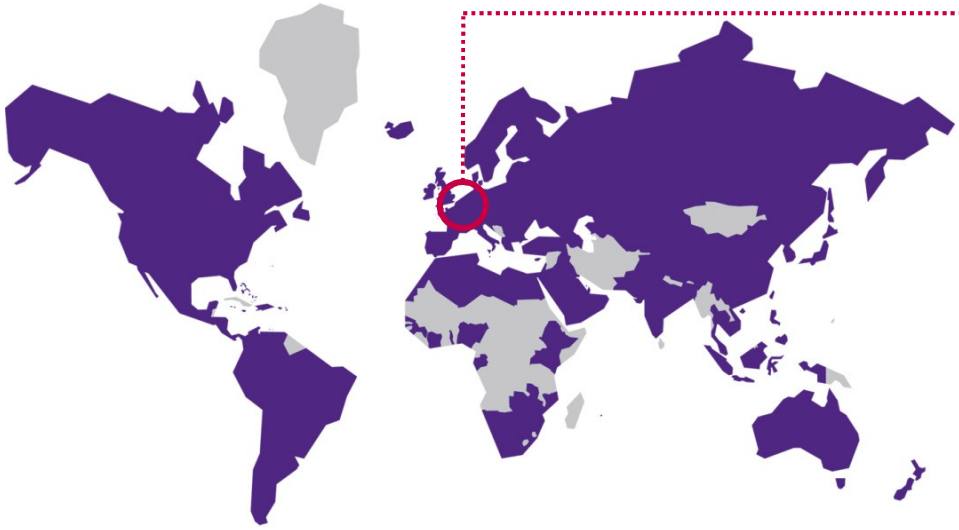
AmCham, InterBilanz, Warth & Klein Grant Thornton
Bratislava/Budapest, March 2016

Global presence for your challenges and requirements

Grant Thornton at a glance

Grant Thornton International Ltd.

- Grant Thornton International is one of the world's leading organizations of independent assurance, tax and advisory firms with an annual combined turnover of US $4.5 billion
- We are where you are:
  Grant Thornton is represented in all major global centers with over 40,000 employees in 134 countries and 700 locations worldwide.



Warth & Klein Grant Thornton AG

- German member firm of Grant Thornton International Ltd.
- Turnover of € 87.4 million.
- 80 partners, a total of approx. 700 employees.
- 10 Offices in Germany.

TOP 3 Wirtschaftsprüfer Markt — 1. PLATZ Kompetenz Wirtschaftsprüfer Markt

THOMSON REUTERS

Ranked most active corporate finance adviser 2012 (Thomson Reuters Small Cap)

top 25 most admired companies 2012

Private Client Practitioner Top 25 Most Admired Companies 2012, 2011, 2010

International Accounting Bulletin 2013 WINNER NETWORK OF THE YEAR GRANT THORNTON

International Accounting Bulletin Network of the Year 2013

Personal introduction

Helmut Brechtken

- Associate Partner, Diplom-Physiker, ISO 27001 Lead Auditor
- Cybersecurity, IT-Forensic, eDiscovery, Data Analytics
- Leadership for more than 100 cases in the area of investigation - focus on: Incident Response Investigation, Forensics, eDiscovery, Cybercrime, Data Leakage
- 6 years of experience at KPMG, Forensic Technology
- 12 Jahre years of experience at Evonik (Degussa): C-level management, Data Center, Cybersecurity, Inhouse Consulting

Warth & Klein Grant Thornton

An instinct for growth™

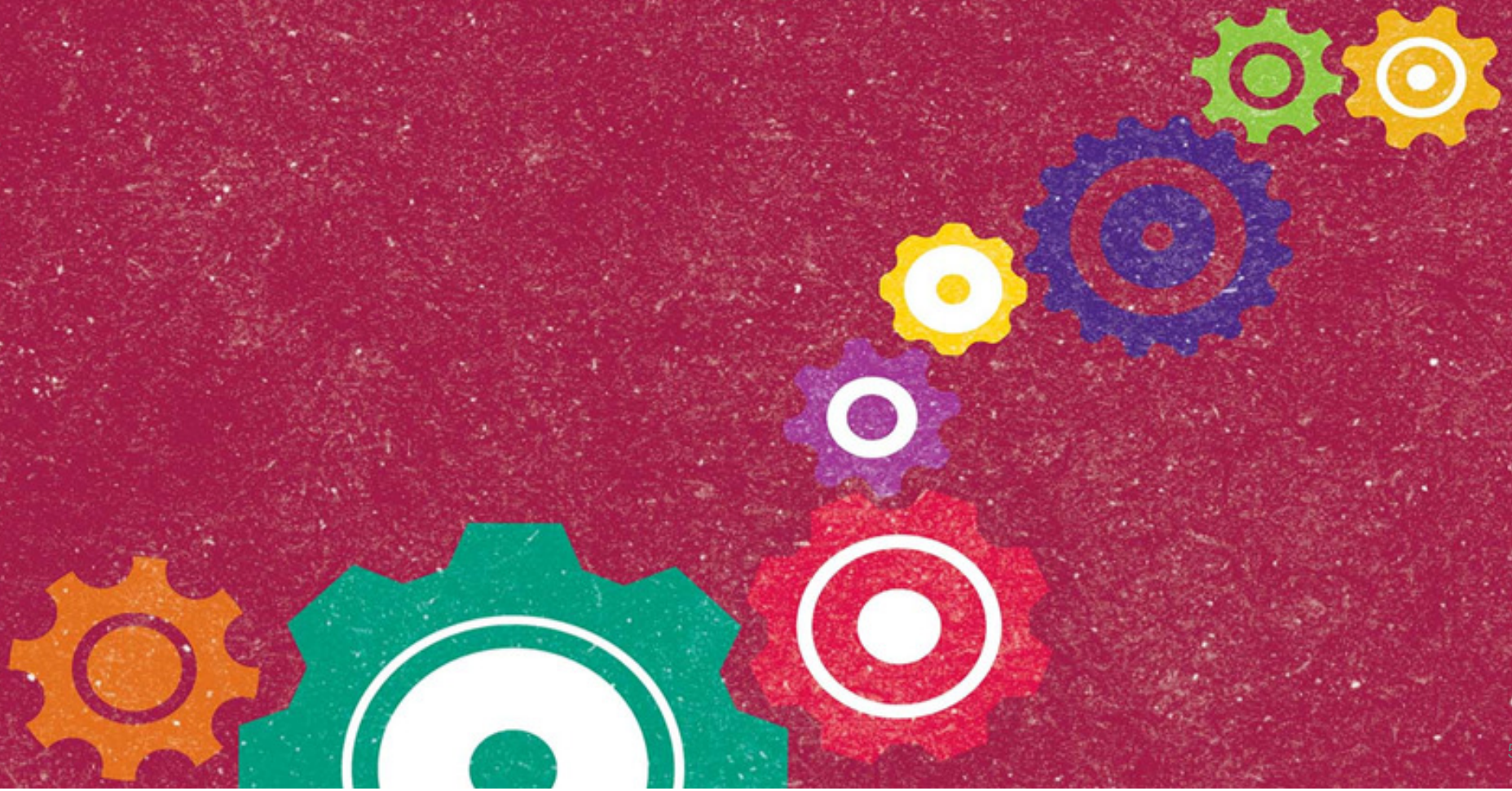
Agenda

1. **Introduction**
2. **Current situation related to Cyber**
   - Statements
   - Studies
   - Statistics
3. **Cybercrime examples**
   - Phishing
   - Ransomware
   - Intrusion
   - Sabotage
4. **Cybersecurity approach**
   - Reactive
   - Proactive
5. **Conclusion**

Warth & Klein Grant Thornton

An instinct for growth™

Current situation in the area of IT-Security and the related consequences for enterprises



Current situation & perception of Cyber Security (1/2)

International press statements

- 8 May 2015 – **UK GOV Security policy**:
  …categorized cyber attacks as a Tier One threat to our national security, alongside international terrorism…

- 12 Dec 2015 – **Obama Signs Cybersecurity Law**:
  …$1.1 trillion spending package for Cybersecurity that funds the government through September 2016…

- 19 Oct 2015 – **French Prime Minister** (Manuel Valls) by launching national cyber-security strategy:
  … Cyberspace has become a new domain for unfair competition and espionage, disinformation and propaganda, terrorism and criminality…

- 19 Nov 2015 – **DEU Federal Minister of the Interior** (de Maizière):
  …ALL companies have to realize that there are cyber attacks against their IT infrastructure…

Current situation & perception of Cyber Security (2/2)

- Disclosures by Edward Snowden:
  - Surveillance (e-mail),
  - Espionage within the industry,
  - Surveillance projects seem to be standard procedures… even among partner states

- Cyber-Attacks
  - Increase constantly
  - Getting more multifaceted
  - Conducted/funded by large organizations
  - Targeted and very complex (Stuxnet)

- Awareness for IT-Security is constantly increasing in all area: Industry, society, politics (IT-Security laws)

Germany: Top 10 enterprise risks in 2015

1		Logistics	55%
2		Cybercrime	32%
3		Legal changes	28%
4		Natural disasters	23%
5		Reputation risks	16%
6		Increasing competitors	15%
7		Economic stagnation	15%
8		Fire, explosion	13%
9		Political-, social change	13%
10		Product quality failures	9%

Source: Allianz Risk Barometer 2015, Allianz Global Corporate & Speciality

Allianz Risk Barometer 2016

Top 10 business risks for business in Europe

Top 10 business risks			2015 Rank	Trend
1	Business interruption (incl. supply chain disruption)	53%	1 (44%)	-
2	Market developments (volatility, intensified competition, market stagnation)	52%	NEW	▲
3	Cyber incidents (cyber crime, data breaches, IT failures)	40%	5 (17%)	▲
4	Changes in legislation and regulation (economic sanctions, protectionism)	39%	4 (20%)	-
5	Macroeconomic developments (austerity programs, commodity price increase, inflation/deflation)	31%	NEW	▲
6	Natural catastrophes (storm, flood, earthquake)	31%	2 (28%)	▼
7	Loss of reputation or brand value	29%	7 (15%)	-
8	Fire, explosion	22%	3 (27%)	▼
9	New technologies (impact of increasing interconnectivity and innovation)	19%	NEW	▲
10	Political risks (war, terrorism, upheaval)	17%	8 (13%)	▼

Source: Allianz Risk Barometer 2016, Allianz Global Corporate & Speciality

Allianz Risk Barometer 2015

The most important risks for businesses in Hungary

Top 10 business risks for Hungary			2014 Rank	Trend
1	Fire/explosion	65%	1 (41%)	-
2	Business interruption and supply chain	52%	3 (28%)	▲
3	Natural catastrophes	48%	6 (21%)	▲
4	Cyber crime, IT failures, espionage, data breaches	13%	NEW	▲
5	Theft, fraud and corruption	13%	4 (23%)	▼
6	Loss of reputation or brand value (e.g from social media)	13%	9 (10%)	▲
7	Terrorism	9%	10 (8%)	▲
8	Pollution	9%	NEW	▲
9	Political/social upheaval, war	9%	NEW	▲
10	Credit availability	9%	NEW	▲

Source: Allianz Risk Barometer 2015, Allianz Global Corporate & Speciality

Latest examples for cyber attacks

Affected side	Occurrence	Date	Damage
US personnel administration (OMG)	**On-going attack for several month: Information exposure and data leakage**	Jun 2015	Around 4 Mio. datasets of US employees working in administrative bodies (incl. Army, CIA, NSA) have been exposed.
German Bundestag	**Hacker gains control of the whole IT-network of the German Bundestag**	Jun 2015	Hacker got access to more then 2000 network devices in the German Bundestag. It was only detected after the attackers started to copy a massive amount of data. After 5 weeks of investigation the administration admitted that the whole network has to be rebuild from scratch. It is still unclear what information have been exposed.
Ashley Madison	**Hacker took control over the customer database of the bank as well as the website with more than 37 Mio. customers**	Jul 2015	Huge financial and reputation damage. Hackers threaten the bank to shut down the online portal or all customer data will be published.
City of Ivano-Frankivisk Oblast, Ukraine	**Total power outage, no electricity due to a malware infection**	Dec 2015	80,000 customers (business and private) in the region were affected
Hospital in the city of Arnsberg, Germany	**Denial of service attack against the hospital IT-infrastructure**	Feb 2016	Due to the outage of the whole IT-system, all staff in the hospital had to go back to „pen & paper“. Not all patients could be handled in time. New patients had to be refused.

Cyber incident examples

Example (1/4): Phishing & Ransomware

Scenario:

- E-mails …, you are requested to open an embedded URL or attachment (malware) to visit a prepared (fake) website
- These sites look exactly the same like: eBay, PayPal, amazon, your trusted bank or your telecommunication provider

Phishing:

- Forcing you to input your account- and password details in order to initiate $cash$ transactions

Ransomware (current attacks on medical centres in Germany)

- Pushing you to visit a website with malware attached
- Malware encrypts all your data (and all accessible company data as well!) and
- Extort $cash$ from you for decryption

- ➢ Often it is a "fake-bad"(language, style, linked to a different site) and will be identified by the majority, but…
- ➢ Lack of quality compensated by massive attacks
- ➢ Continuously evolving in technique and style – harder to detected

Example (2/4): Project „Order“: President Fraud

President Fraud:

- You are the CFO or work in the financial department responsible for transactions
- You receive an e-mail from your CEO or president
- The style of this e-mail is according to cooperate identity, including signature etc.
- E-mail content & language style fits exactly
- Requests you to perform $cash$ transactions to foreign countries (strictly confidential and extremely urgent)

- ➢ Cyber criminals prepare their targeted attacks very well by in-depth background research and social engineering
- ➢ Quality of these attacks are very high – frequent is fairly low

Example (3/4): Project „Midnight“: Network intrusion

Financial sector:

IT network (Bank) has been compromised. Specialists realized that the attacker was in the network already since 57 hours

- **How could this happen?**

  Access through a weakly configured VPN-Tunnel. Only one single (shared) access-account using a static password (~ 1 factor, but static).

- **Where did the attack come from?**

  Some evidences led to a web-hoster within the USA. Even with an international offence report further tracing remained unpromising

- **What system or data have been compromised?**

  Available traces have been analyzed and affected system were identified: After hacking an internal account the intruders had access to various systems (R&D, Webserver, Knowledge Base, **operational systems with access to the central account-database of the bank**)

Example (3/4): Project „Midnight“: Network intrusion

- **What data has been extracted?**

  A detailed analysis of the log-files to reengineer the attack clarified:

  - Multiple attempts to copy the whole content of the database
  - Fortunately, attempts remained unsuccessful due to a lack of knowledge about the necessary programming language (SQL-Queries „select * from ….. where ……“)

- **Conclusion:**

  Close to “worst case scenario” – indication to the UK FSA (Financial Services Authority) would have been mandatory incl. serious consequences: Information to all customers, official forensic investigation, potential loss of the banking license

Example (4/4): Project „X“ – internal sabotage

Project „X“

- Industrial company, around 350 employees, raw materials
- 13 incidents reported / interferences with the IT network in April – August 2013
  - Outage: Fileserver (2x)
  - Outage: Logistic software (3x) (around 2 Mio € fin. damage /day)
  - Massive malware attack(> 300 viruses identified)
  - MS Windows AD (Domain has been renamed – 1 Tag outage)
  - Hardware failure at the domain controller
  - Manipulation within the surveillance system (video) in the server room
- Some incidents required internal support (sabotage)

➢ Forensic Investigation

Example (4/4): Project „X“ – internal sabotage

Plan of investigation:

- Corporate Intelligence / background research (~ 5 companies, 20 players)
- Internal information gathering
- Personal dialogs to inform the staff and forensic interviews
- IT-Forensic analyses (technical)
- Profiling

➢ Upcoming approach: Undercover investigation

Example (4/4): Project „X“ – internal sabotage

Project progress (September 2013 until March 2014):

- Project Team on-site, steering committee, coordination with RA, DSB, BR
- CI: no noticeable abnormality
- Information gathering, detail asset description led to following results:
  45 incidents confirmed, 7 could explicit classified as internal sabotage e.g.:
  - EMC SAN logically destroyed
  - Logistic System: OS-HD deleted from 3 Servers
- **BIG DATA**: 26 HD incl. digital evidences (11 incidents – TMI)
- Detailed IT forensic analyses for 5 incidents with the highest priority
- 20 forensic interviews – official / undercover
- Profiling: completed

Example (4/4): Project „X“ – internal sabotage

Final conclusion / results:

- No incidents for 5 months
- **Than, an additional incident occurred:**
  - Suspect could be identified
  - Identification via „IP Trap“
  - Consequences for the suspect: legal consequences by the employer, official criminal complaint, claims for damages
  - Consequences for the company: „deliverance“, situation was tensed up for a long period (internal loss of thrust…)

Example (4/4): Project „X“ – internal sabotage

Addition findings / recommendations:

- **Incident Response Plan**
- **Potential for improvement / optimization:**
  - **Organizational** (4 Player, several consultants):
    - Roles & Responsibilities
    - Communication
    - Procedures
    - Policies & Guidelines
  - **Technical**
    - IT-Security (account management, passwords)
    - Anti-virus
    - Patching
    - Backup

Governance, Risk & Compliance

Cybersecurity counter measures

Cyber Security services (1/2)

Cyber Compliance **„full control over IT-Security & compliance“**	▪ **Cyber compliance, audits and certifications :** Audits according to ISO/IEC 27001, BSI Grundschutz, ISIS12, migration testing, Software-assessments ▪ **IT-Security-Law-Compliance:** Consultation to meet the legal requirements and periodical / frequent audits ▪ **Protection of privacy**: Audits with regard to the protection of data privacy and hosting the role of an external data security official / data protection officer
Cyber Response **„knowing what to do in case of crises and attacks“**	▪ **Cybercrime & Incident Response Investigation:** IT-forensic investigations to analyze IT-Security incidents like: Hacker attacks, data leakages incl. immediate closure of security vulnerabilities, evaluation of the damage (financial and technical) and back tracing of the attacks ▪ **Incident Readiness:** Consultation regarding the organization, infrastructure, processes and procedures, to be able to respond quickly and precise according to the predefined policy in case of an IT-Security incident ▪ **Disaster Recovery & Business Continuity:** Development of detailed plans and procedures, crises-exercises, support to conduct data and system recovery

Cyber Security services (2/2)

Cyber Prevention **„Prevent by using security methods“**	▪ **Cybercrime Prevention:** Risk assessment und audits of the IT-Security-organization, processes and procedures, existing security measures (technical & procedural), Web App & Wi-Fi, Pentest and awareness trainings ▪ **Code Reviews:** Review of software code for any weaknesses and vulnerabilities, back-doors, malware (Trojan...) ▪ **Industry 4.0 security aspects:** Consulting with regard to the implementation of a defense-in-depth security concept to protect sensitive industrial facilities and installations
Cyber Attack **„Learn by any incidents occurred“**	▪ **Pentesting (Black/White):** Assessment to analyze the current level of security by simulating internal and external attacks on the IT-infrastructure incl. Wi-Fi (with /without involvement of the local IT-department) ▪ **Web Application Check:** Security assessment of Web-applications (web-stores,..) ▪ **Social Engineering:** Assessment of the awareness of all employees by using various social methods to acquire sensitive information ▪ **Physical security:** Assessment of the physical security by specific and targeted attempts to get physical access (direct or via work-arounds) to installations

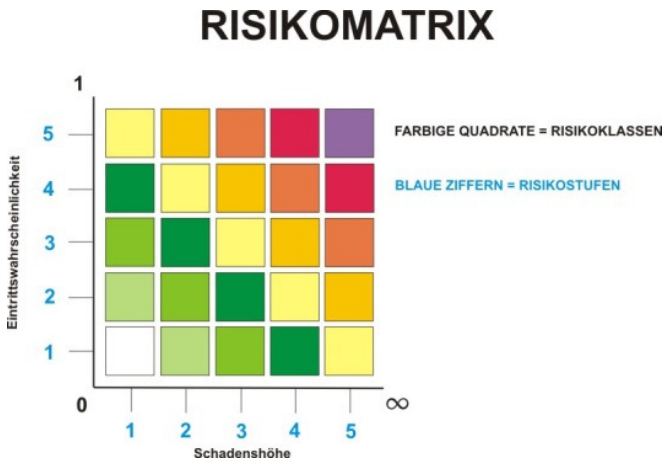
Improvements for Cyber Security services

1 Assessment of the „current state“:

1. Risk- / requirement analysis
2. Review of the IT-organization, IT-processes und IT-environment to identify any vulnerabilities
3. Pentests (external and internal) against all IT-systems incl. Wi-Fi, VPN, mail,..
4. Security awareness training for management and staff

2 Selection and implementation of appropriate (technical and financial) measurements to achieve a secure IT-environment

3 Regular reviews (at least every 2 years)



Governance, Risk & Compliance

Conclusion

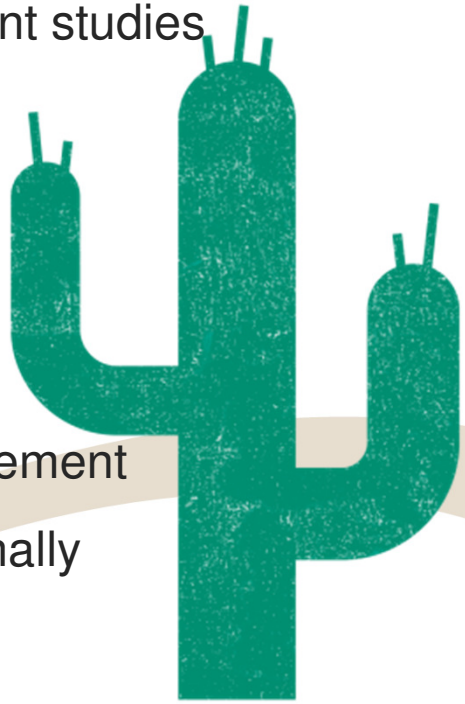
Conclusion

Current Situation

- There are many new threats arising due to business dependencies on IT
- The situation is obscure and there is no clear status available
- Importance for cyber is rising around the globe according to recent studies

What now?

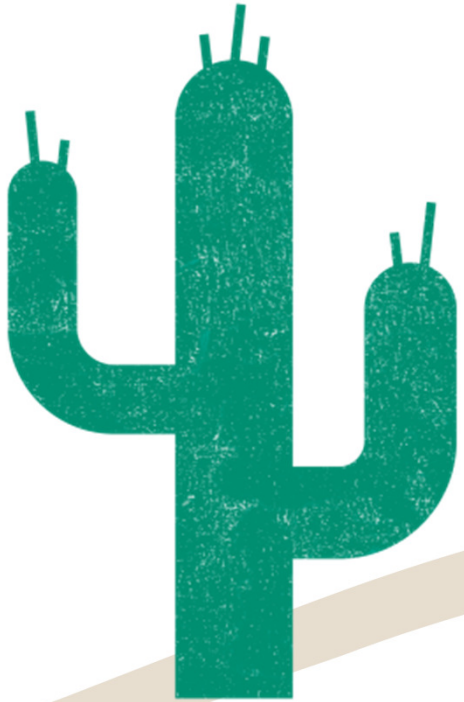
- Put your attention on cyber
- Do not ignore the phenomenon because of it‘s ascertainablity
- Accept advice, initiate the necessary actions and control measurement
- Let your IT-organisation, -processes and -infrastructure be externally reviewed on a regular basis



Thank you for your attention

Warth & Klein Grant Thornton

An instinct for growth™



Warth & Klein Grant Thornton AG
Wirtschaftsprüfungsgesellschaft

Warth & Klein Grant Thornton AG is a member of Grant Thornton International Ltd (Grant Thornton International).

The name Grant Thornton refers to Grant Thornton International or one of their member companies. Grant Thornton International and the member companies are no worldwide partnership. Each member provides it's service autonomously and independent from Grant Thornton International or other members.

wkgt.com