EVENTUS

Consulting

Counter measures against
economic crime, fraud & industry espionage

March 2020

Content

Partners

MAZARS

Globally active professional services firm with 24,000 employees in 89 countries and yearly revenues (2018) of more than EUR 1.6 bn.

Successful track record of covering corporate and government clients in strategic projects.

Unique synergies are created by EVENTUS security expertise and MAZARS top level consulting know-how.

Innovative services protect from economic crime and allow our clients to react in the right way to incidents.

ÖWD

RESULT GROUP
Global Risk and Crisis Management

INNOTRONIC

TABAK FABRIK LINZ

AMEYA

Stratfor

AVANTGARDE
INTERNATIONAL PROPERTIES

CHRISTIE'S
INTERNATIONAL REAL ESTATE

ARES
preventing leaks

Threats

Economic Crime, Fraud and Industry Espionage

€ 5-6 bn.

annual damage to Austrian companies due to economic crime, fraud and industry espionage.

5 %

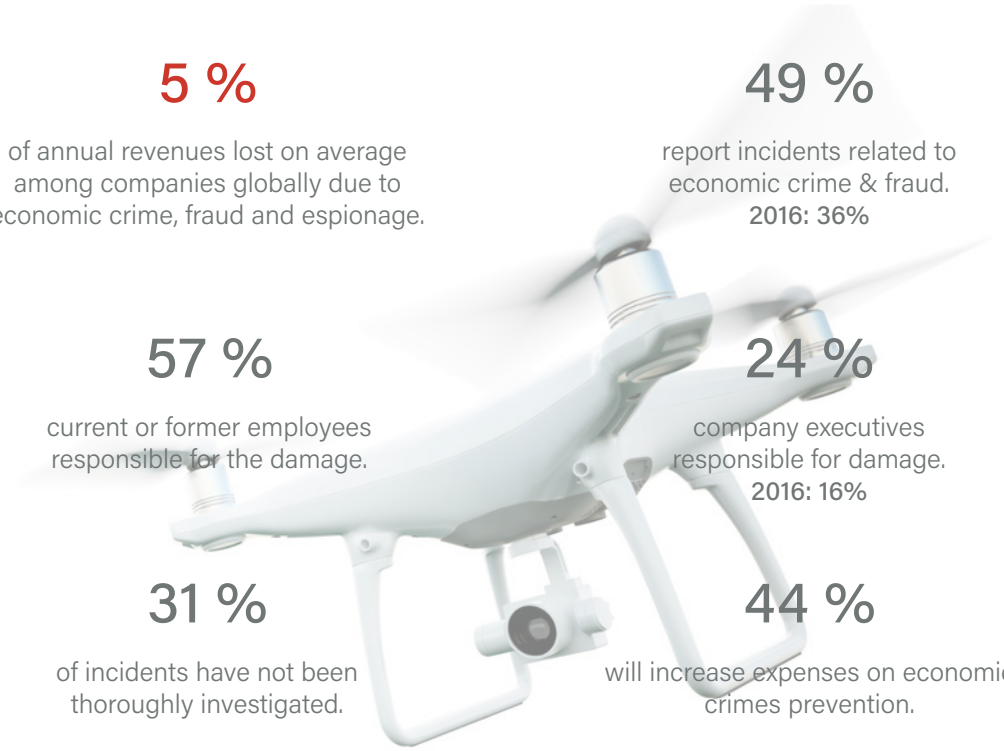
of annual revenues lost on average among companies globally due to economic crime, fraud and espionage.

49 %

report incidents related to economic crime & fraud.
2016: 36%

52 %

internal perpetrators responsible for damage.
2016: 46%



31 %

of questioned companies have fallen victim to industry espionage.

57 %

current or former employees responsible for the damage.

24 %

company executives responsible for damage.
2016: 16%

68 %

of external perpetrators are frenemies, i.e. agents, external service providers, suppliers and clients.

85 %

of the companies are unaware of preventive measures.

31 %

of incidents have not been thoroughly investigated.

44 %

will increase expenses on economic crimes prevention.

46 %

have not evaluated the risks related to economic crime.

BM.I BUNDESMINISTERIUM FÜR INNERES

FH CAMPUS WIEN UNIVERSITY OF APPLIED SCIENCES

ACFE Association of Certified Fraud Examiners

WKO

iv INDUSTRIELLEN VEREINIGUNG

pwc

Legal Framework

Companies must implement preventive security and confidentiality measures:

Contractual

Confidentiality agreements, competition clauses etc.

Organisational

Documentation, policies, guidelines, processes etc.

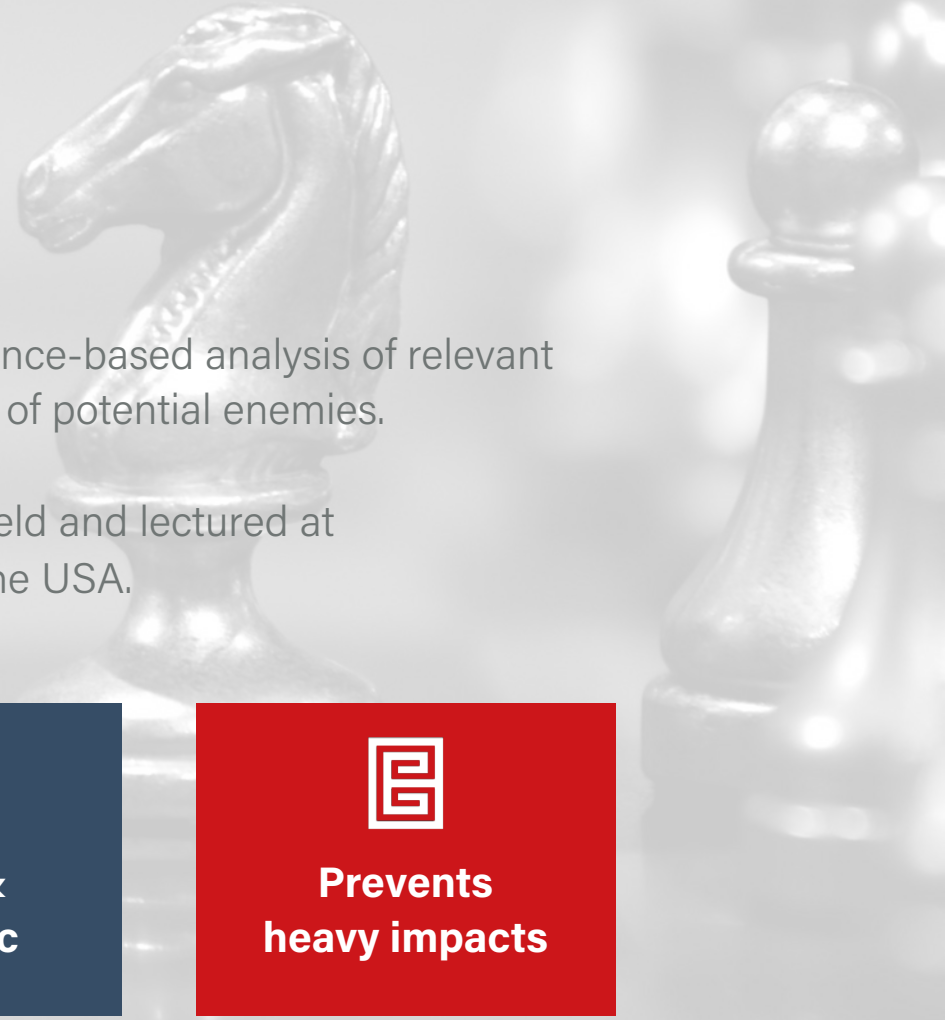
Technical

Entrance barriers, cyber security, encryption etc.

Legal protection and enforceability only in case of adequate as well as preventive security measures.

Directive (EU) 2016/943 on the protection of undisclosed know-how and business information

Strategic Scenario Mapping

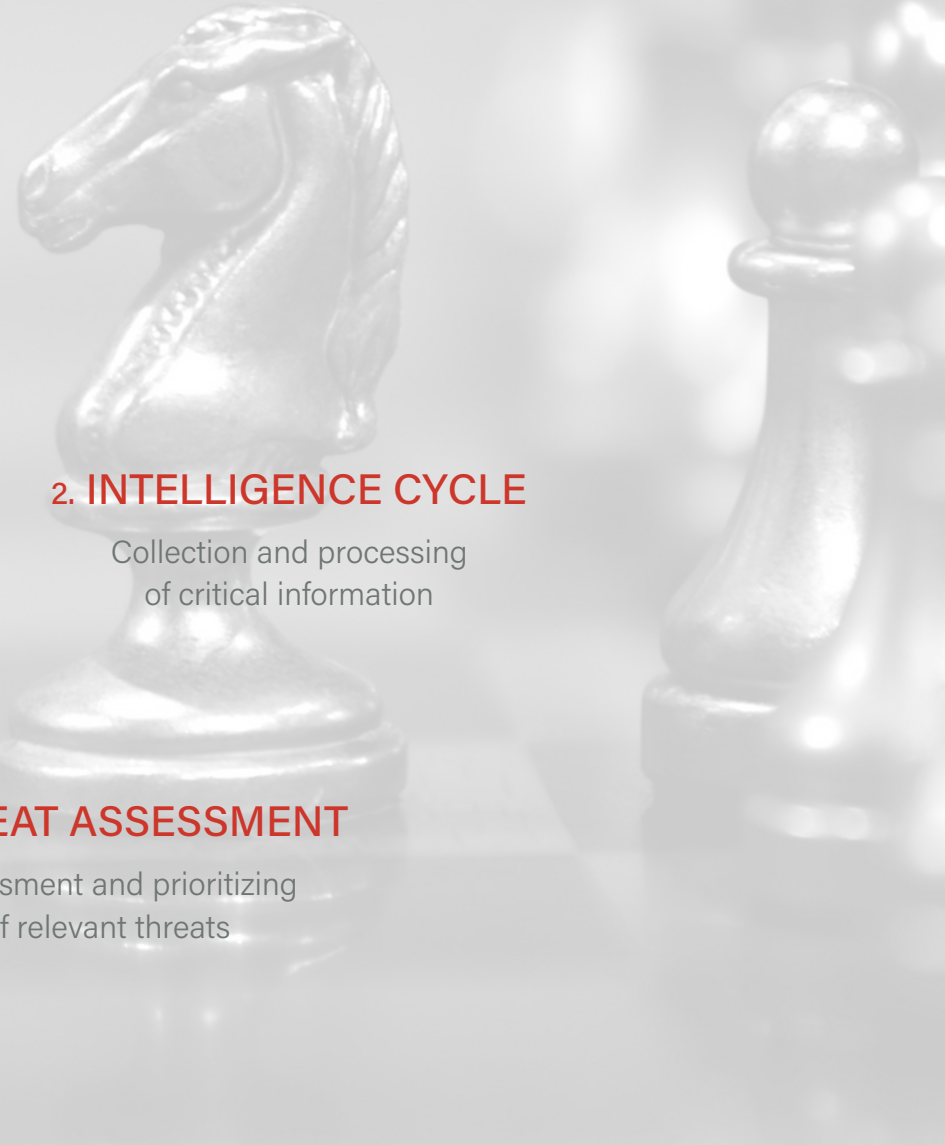


Our unique Strategic Scenario Mapping © approach offers intelligence-based analysis of relevant players and scenarios taking into account the perspective of potential enemies.

SSM has been successfully applied during missions afield and lectured at Special Operations schools in Austria and the USA.

✓ **Targeted focus**	✓ **Proactive vs. reactive**	✓ **Explicit & systematic**	**Prevents heavy impacts**

SSM Cycle



1. MISSION ANALYSIS

Definition of the assignment's target parameters

2. INTELLIGENCE CYCLE

Collection and processing of critical information

3. THREAT ASSESSMENT

Assessment and prioritizing of relevant threats

4. SCENARIO DEVELOPMENT

Wargaming and definition of recommended actions

5. MISSION EXECUTION

Implementation of necessary measures

STRATEGIC SCENARIO MAPPING

ssm

Cyber Security

72 % of surveyed companies believe that awareness deficits are the highest risk for the cyber security of a company.

Only 28 % think that missing or outdated technology is the biggest challenge.

Top 3 Business Risks

1. Cyber incidents
2. Business interruption
3. Legislation & regulation

Global Risk Barometer 2020

To protect your organisation is critical - attacks are frequent and different in nature.

Independent of the type of attack, the main motivation of criminals is mostly to make money.

Organisation

- Security Awareness workshops for executives and employees
- Cyber Security trainings
- Social Engineering defence mechanisms
- Adequate Controls & Procedures

Technology

- Vulnerability Analysis
- DNS Umbrella – Made in Austria
- Data Protection solutions
- Penetration Tests
- Risk Scenario Trainings

Perspective

- Protective Intelligence Analysis
- Understanding of attack cycle of potential enemies – internal, external & hybrid
- Cyber attacks are merely one of many tools of sophisticated attackers

Virtual Terrain

DNS Umbrella – Made in Austria

- Based on Big Data, Machine Learning and Artificial Intelligence
- Blocks all types of attacks in real-time
- Additional protection for mobile devices
- Integration in existing IT infrastructure
- 20 minutes: easy and quick installation
- 30 day free trial: all attacks blocked and listed in a dashboard
- GDPR compliant
- Reference clients:

UNSER HEER
WIENER STÄDTISCHE Vienna Insurance Group
JKU Johannes Kepler Universität Linz
STRABAG
HOFBURG VIENNA
VKB | BANK

Voice Biometric with AI – Made in UK

- Artificial intelligence optimises the performance over time
- Many use cases: KYC, AML, GDPR, PSD2 etc.
- Protect the identity of your clients or patients
- Management of internal access rights
- Easy integration thanks to existing API and SDK
- Mobile apps and on-device identification
- GDPR compliant
- Reference clients:

BARCLAYS
NatWest

Human Success Factor

Not sophisticated hacker attacks are the most imminent threat, but the security awareness of your own employees and executives with regard to the correct behaviour in light of cyber attacks.

Only 39% of executives and employees have already participated in a cyber security workshop.

YouGov / GDV 2019

Companies must educate their employees with the help of adequate organizational development provided by professional services firms.

Social Engineering

poses the highest risk for organizations of all sizes – independent of technology use.

Employees are the key

to effective economic crime, fraud and industry espionage prevention.

43.5 % vs. 1.1 %

far more incidents detected with the help of internal tips vs. technology use.

Report to the Nations, ACFE 2016

Solutions

Protective Intelligence Analysis	Organisational Development	Risk Management	Ongoing Support
• All terrains including Cyber Security • Our unique approach SSM takes into account the perspective of potential enemies • Red Team Simulations • Targeting Profile Estimate • Threat Assessment • Vulnerability & Risk Assessment • Recommendations	• Individual training for executives and employees • Cyber Security workshops • eLearning over existing infrastructure, e.g. Yammer • Technology solutions • Implementation of elevated security standards in the form of Controls & Procedures • Internal Threat Management including the establishment of a reporting system	• Design and implementation of policies and processes • Typical mistakes of standardised check lists are avoided • Emergency Planning • Business Continuity Management • Alternative IT infrastructure for cases of emergency • Scenario training for all involved employees	• Regular Threat Updates • Training for existing and new members of the organization • Physical and virtual Red Team Simulations test and validate existing policies and processes • Establishment of a Rapid Response channel • Signalling to the outside that the own organisation is not an easy victim
Phase 1	**Phase 2** (individual & focussed; builds on Phase 1)		

Contact

Mag. Johannes Glöggler
CEO

+43 676 793 99 48
jhg@eventus-cpi.com

EVENTUS
CONSULTING · PROTECTION · INTELLIGENCE

Eventus-cpi GmbH
Salzgries 17 ▪ A-1010 Vienna

T +43 1 373 65 41-0
F +43 1 373 65 41-33

info@eventus-cpi.com
www.eventus-cpi.com

Olivier Scherlofsky
Partner

+43 664 511 55 84
os@eventus-cpi.com