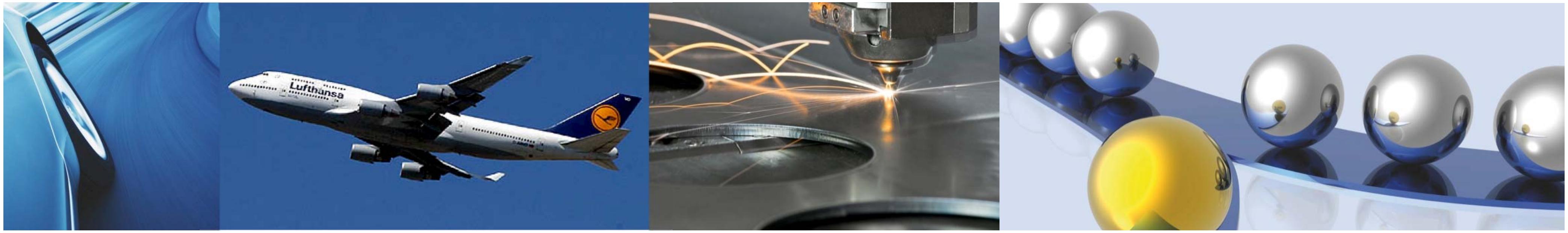


Corporate Security 2030: Challenges & Opportunities
Executive Summary

Klaus Burmeister | Z_punkt The Foresight Company

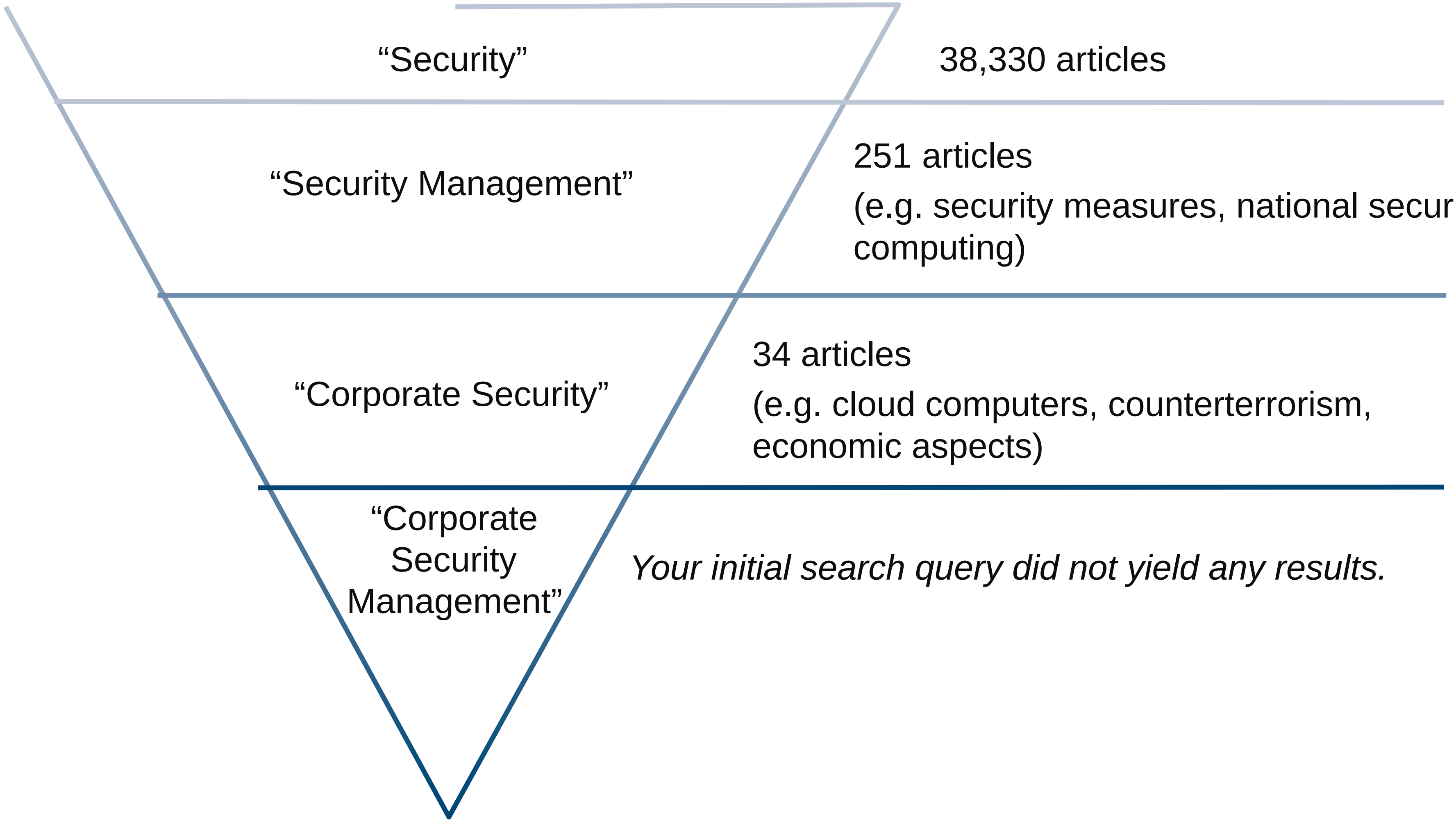
Prof. Dr. Christoph Georgi | EBS Business School

Unter Mitarbeit von:
Björn Theis & Kai-Felix Gülden (Z_punkt The Foresight Company)

März 2015

Inspiring Personalities.

Research on Corporate Security / Corporate Security Management is – by and large – non-existent



“Security” 38,330 articles

“Security Management” 251 articles

(e.g. security measures, national security, computing)

“Corporate Security” 34 articles

(e.g. cloud computers, counterterrorism, economic aspects)

“Corporate Security Management” *Your initial search query did not yield any results.*

EBSCO Host. Query terms in Title or Abstract. Publication Date: 2000–2015 in Scholarly / Academic Journals. Search Date: 11.11.2014.

Security Management is the judicious use of means to accomplish …
… a state of being secure, as freedom from danger, injury, or risk; fear, anxiety, or doubt

- Terrorism, extremism, radicalization

- Crime, economic and industrial espionage

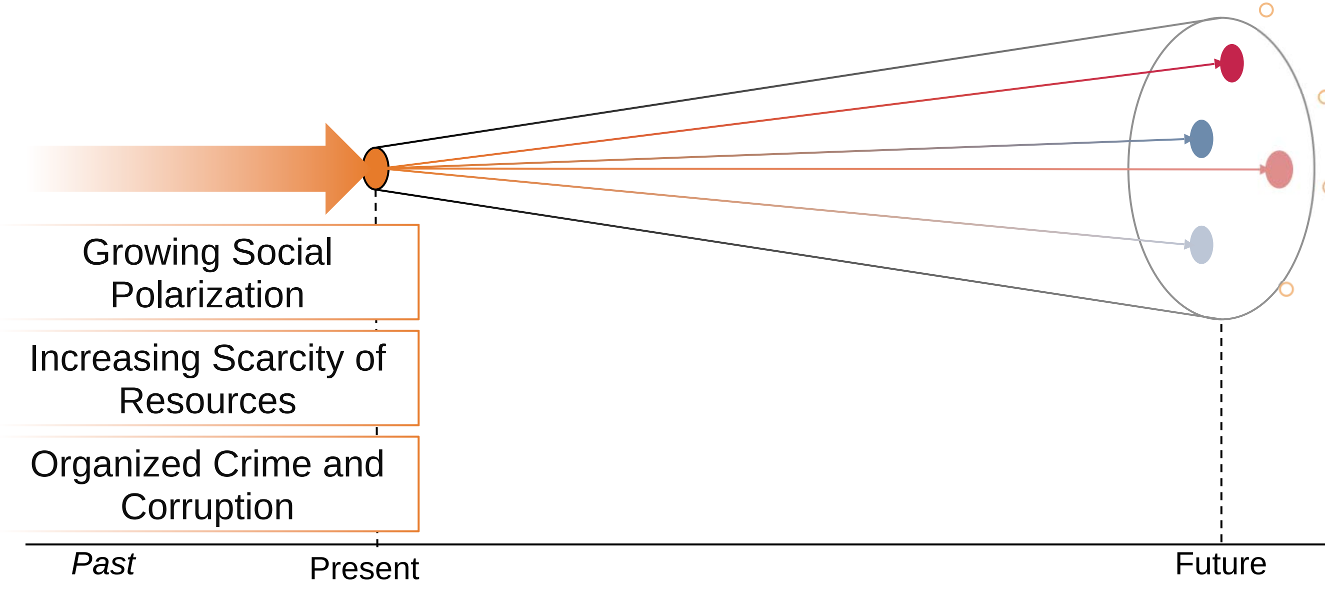
- Natural disasters

- Political, social, and economic instability

Challenges for Corporate Security Management

Security-relevant trends and projections
For which potential futures should Corporate Security be prepared?

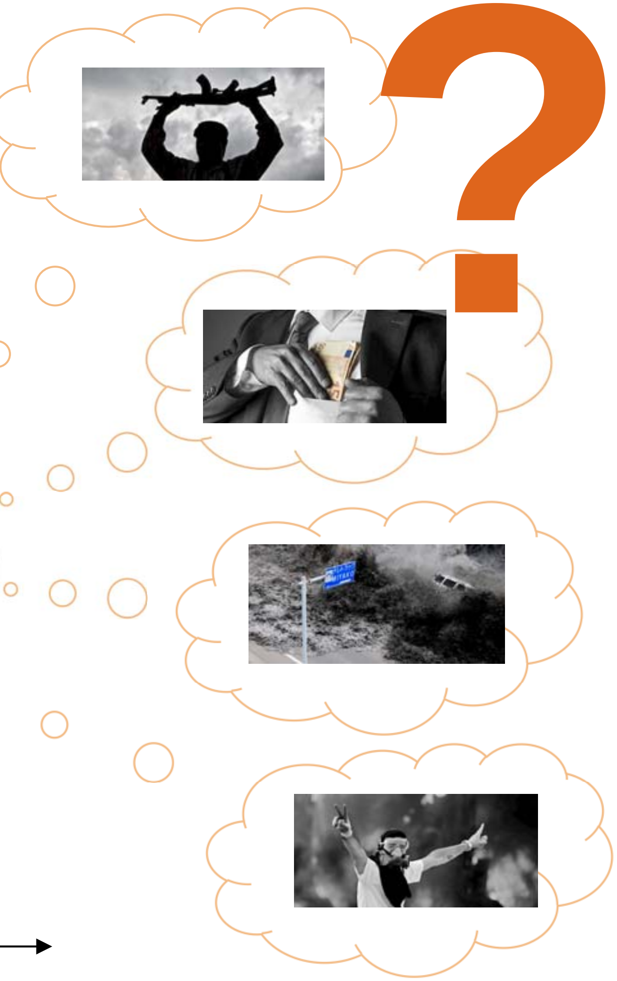
> “ Prediction is very difficult, especially if it's about the future.
>
> *(Niels Bohr, Nobel laureate in physics 1922)*



Growing Social Polarization

Increasing Scarcity of Resources

Organized Crime and Corruption



Inspiring Personalities.

Diverging perspectives

Which potential futures does management consider relevant?

Security’s perspectives

Freedom from danger, injury, or risk

- Protecting employees, facilities and corporate processes around the globe
- Protecting the company's expertise, data and information
- Rapid response and ability to take action in critical events
- Efficient, effective security risk management
- Complying with legal requirements, laws, rules and values around the world

?

Stakeholder’s perspective

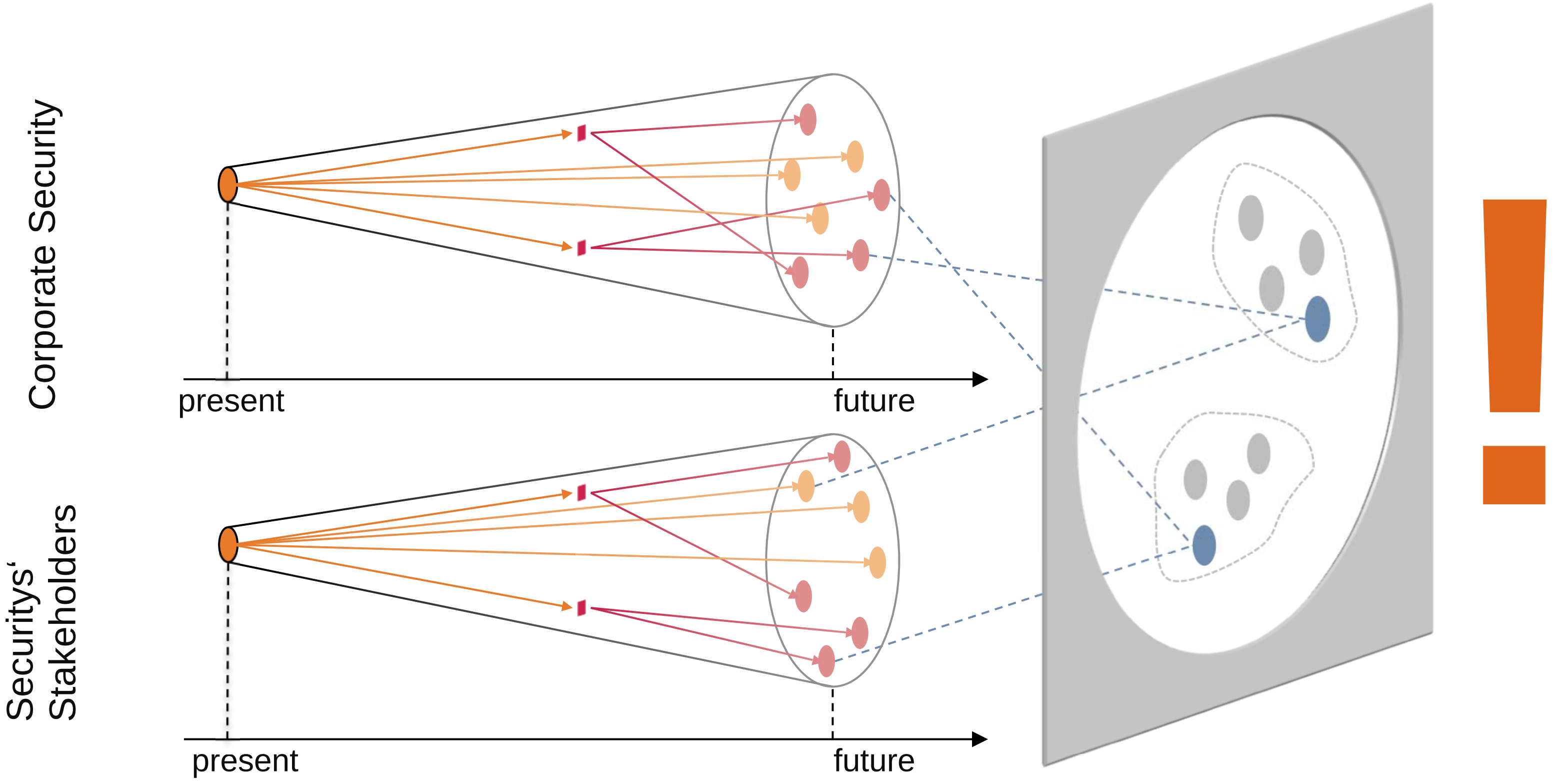
Freedom from fear, anxiety, or doubt

- Expanding the company's global presence
- Changed forms of collaboration on a global level (including joint ventures and partnerships)
- High investments in future technologies and mobility concepts
- Fast pace of technological development
- Increasing requirements for ethics and compliance in the company

„It‘s the business that comes first and justifies the return on investment in protection and security, not the security that would protect the business.“ (Ocqueteau, 2011)

Ocqueteau, F. (2011). Heads of corporate security in the era of global security. *Champ pénal/Penal field*, *8*.

Using Delphi methods, divergent perspectives on potential futures between Corporate Security and its Stakeholders can be quantitatively and qualitatively analysed

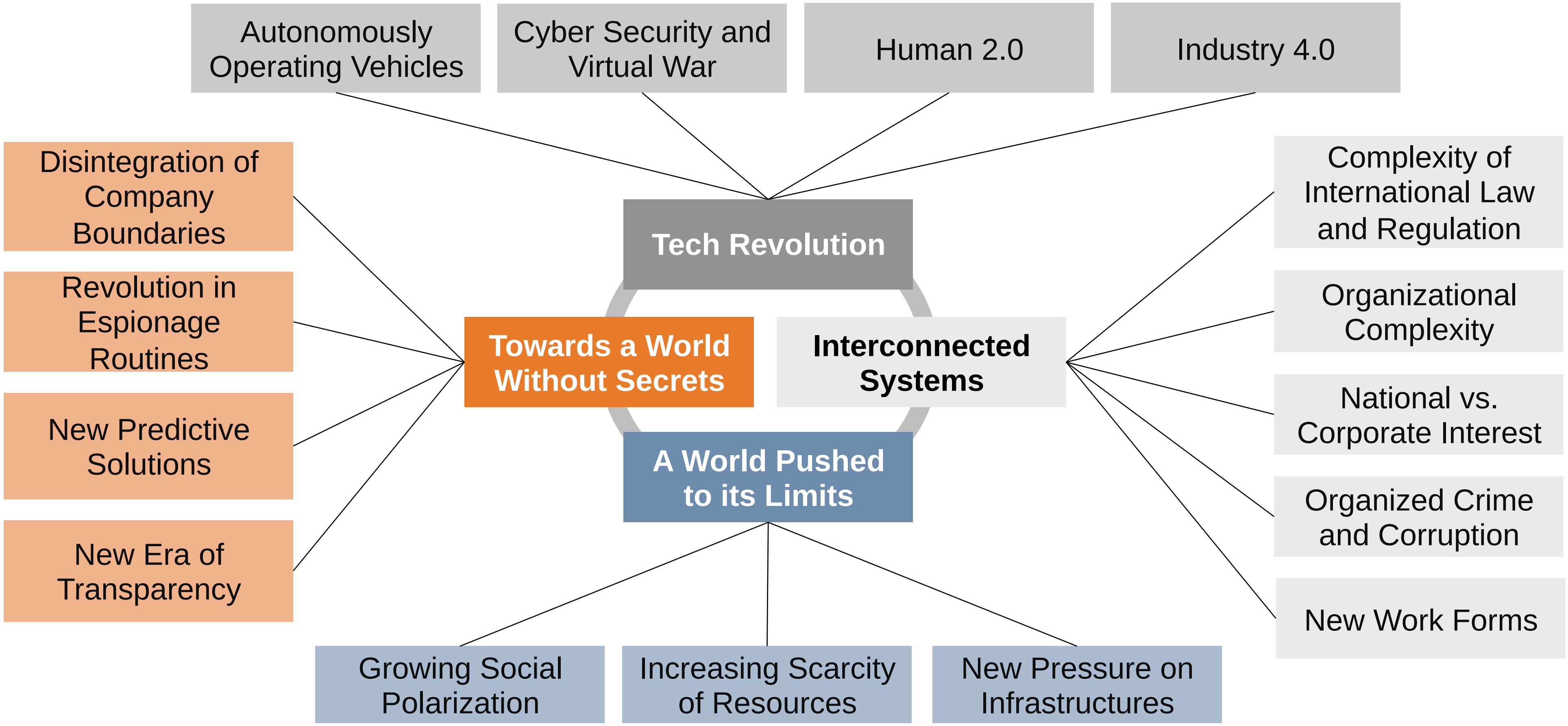


Corporate Security 2030: Research approach
1 – Identify security-relevant changes in the business environment

Identify trends

- What **potential events and developments** can influence the business and its environment and why?
- What **impact** might this have on the company and security?
- What **potential hazards** are associated with it?

16 security-relevant trends grouped in four clusters were identified along the STEEP sectors and described


Autonomously Operating Vehicles
Cyber Security and Virtual War
Human 2.0
Industry 4.0
Disintegration of Company Boundaries
Revolution in Espionage Routines
New Predictive Solutions
New Era of Transparency
Tech Revolution
Towards a World Without Secrets
Interconnected Systems
A World Pushed to its Limits
Complexity of International Law and Regulation
Organizational Complexity
National vs. Corporate Interest
Organized Crime and Corruption
New Work Forms
Growing Social Polarization
Increasing Scarcity of Resources
New Pressure on Infrastructures

Theis, B., & Gülden, K.-F. (2014). *Corporate Security 2030: Challenges & opportunities. Preliminary trend report* [unpublished research report]. Cologne: Z_punkt.

Based on 16 security-relevant trends, preliminary strategic actions for corporate security management were derived addressing major challenges and opportunities

Tech Revolution

- While ever more actions are carried out by autonomously operating machines, it becomes crucial to develop guidelines that give advise on wrongdoings or accidents caused by corporate machinery.
- In addition, corporate security has to monitor and protect M2M communication and activities of autonomously operating vehicles outside corporate borders, in order to prevent information from leaking out.

Interconnected Systems

- Triggered by increasing levels of interconnectedness, harmful cascade-effects (resulting from malfunction or system crashes) bring about the need to work out effective safeguards and counter measures.
- In order to adequately deal with rising complexity levels, security officials need to design security measures from a highly systemic view focusing on system relations rather than on isolated problem solving.
- Due to decentralized structures (e.g. project work) corporate security has to redefine its territory of protection.

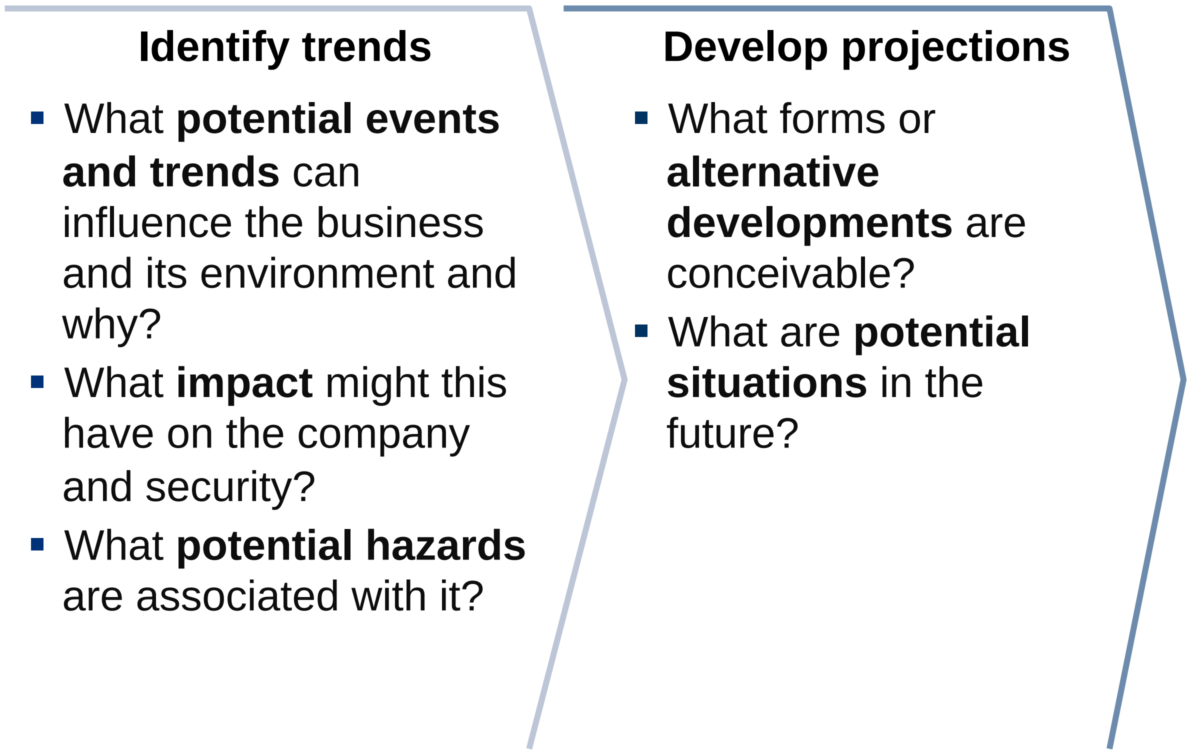
A World Pushed to its Limits

- Within a world that is pushed to its limits, human inhibition is reduced to overstep laws and rules making it necessary for corporate security to step in and provide security where public institutions fail to do so.

Towards a World Without Secrets

- Corporations may have to change their business models radically, as they can not rely anymore on keeping-up their competitive edge through securing information or technology advantages.
- In a world where secrets are hard to keep, redefinition of objects to be protected becomes crucial: Priority shift takes place with regard to the protection of persons creating knowledge vs. corporate knowledge itself.

Corporate Security 2030: Research approach
2 – Develop potential future states



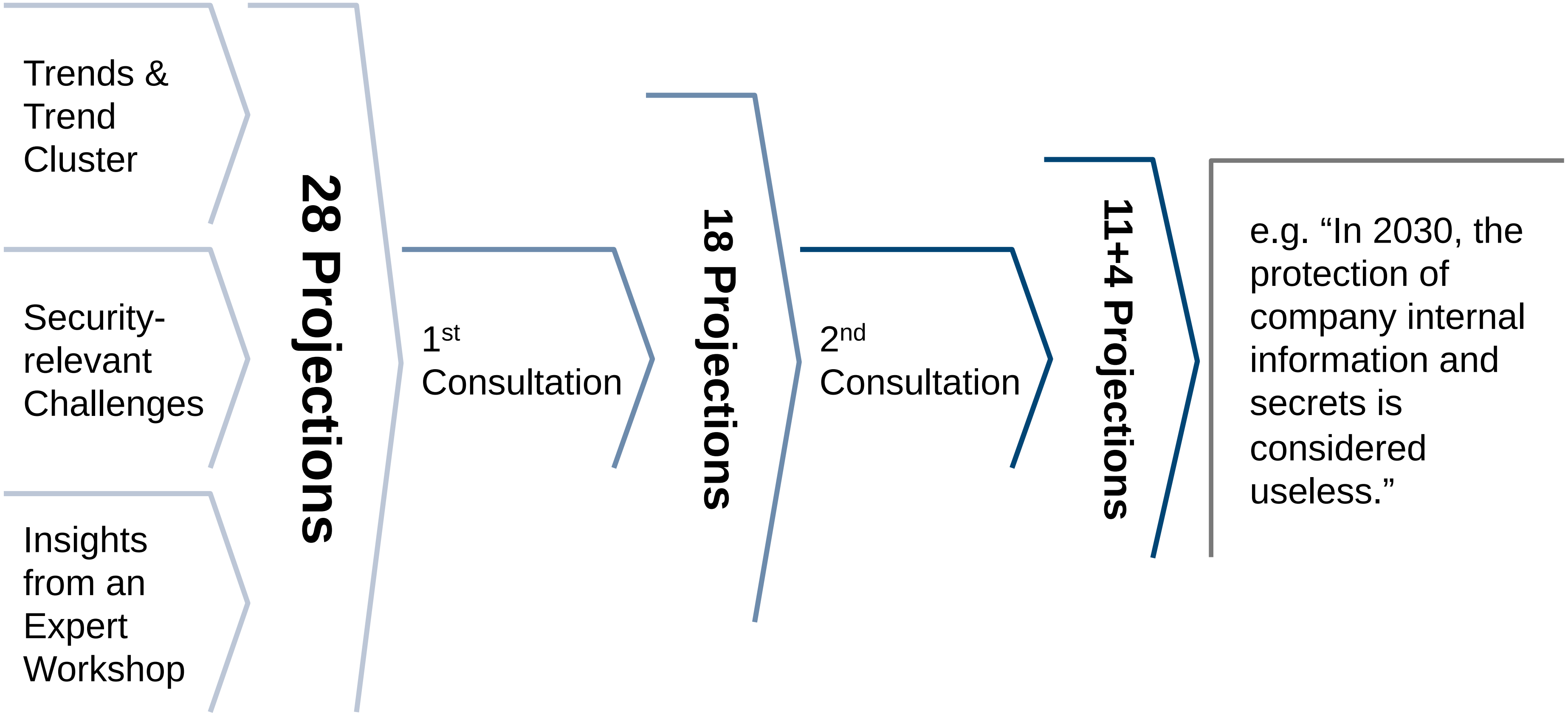
Identify trends

- What **potential events and trends** can influence the business and its environment and why?
- What **impact** might this have on the company and security?
- What **potential hazards** are associated with it?

Develop projections

- What forms or **alternative developments** are conceivable?
- What are **potential situations** in the future?

Based on the four trend clusters and insights from the first Expert Workshop, 28 projections were developed; 11+4 projections were included in the Delphi-Panel



Trends & Trend Cluster

Security-relevant Challenges

Insights from an Expert Workshop

28 Projections

1st Consultation

18 Projections

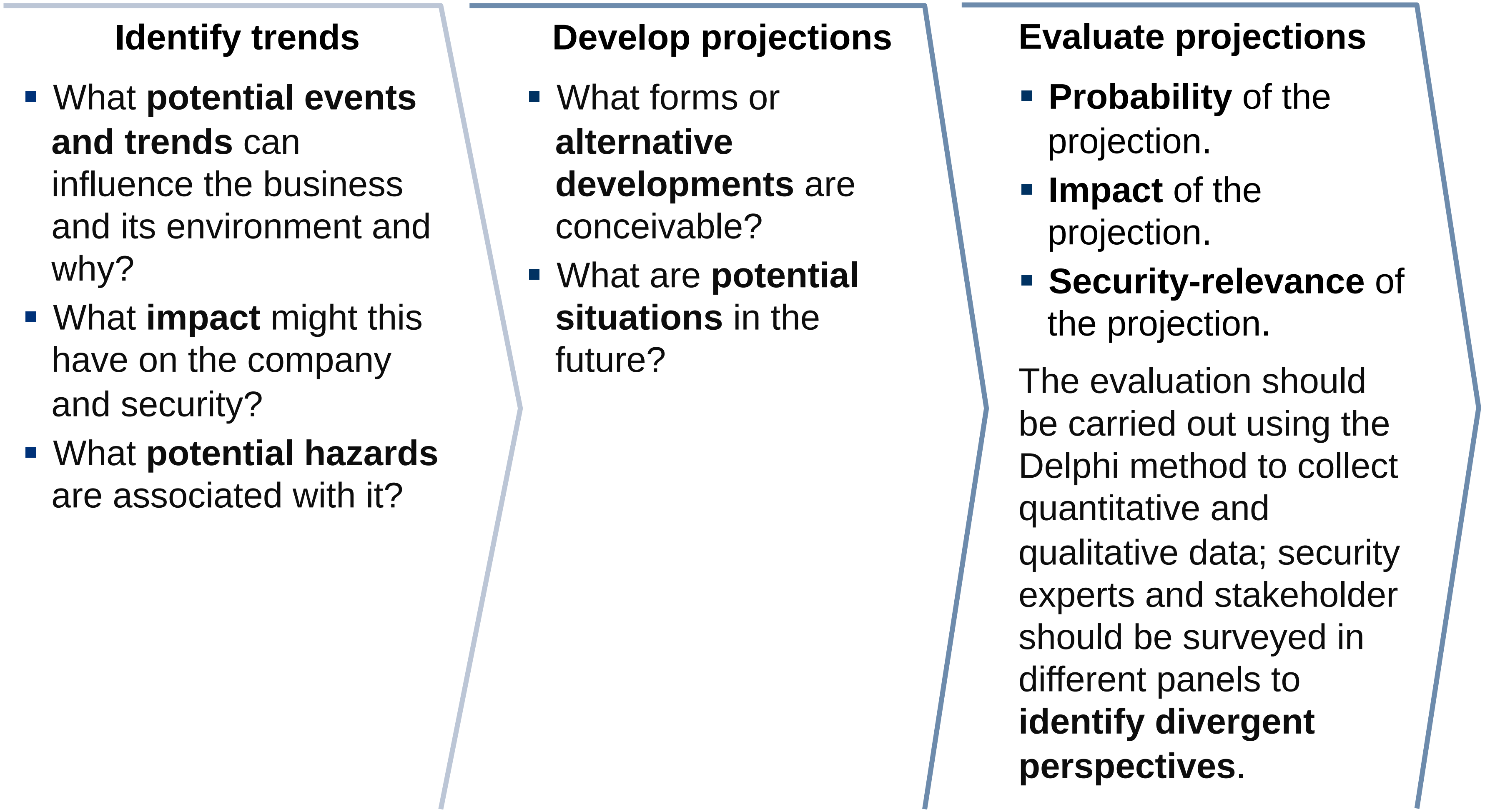
2nd Consultation

11+4 Projections

e.g. “In 2030, the protection of company internal information and secrets is considered useless.”

The Projections are found in Appendix A.

Corporate Security 2030: Research approach
3 – Analyse and evaluate (possibly divergent) future states…



Identify trends

- What **potential events and trends** can influence the business and its environment and why?
- What **impact** might this have on the company and security?
- What **potential hazards** are associated with it?

Develop projections

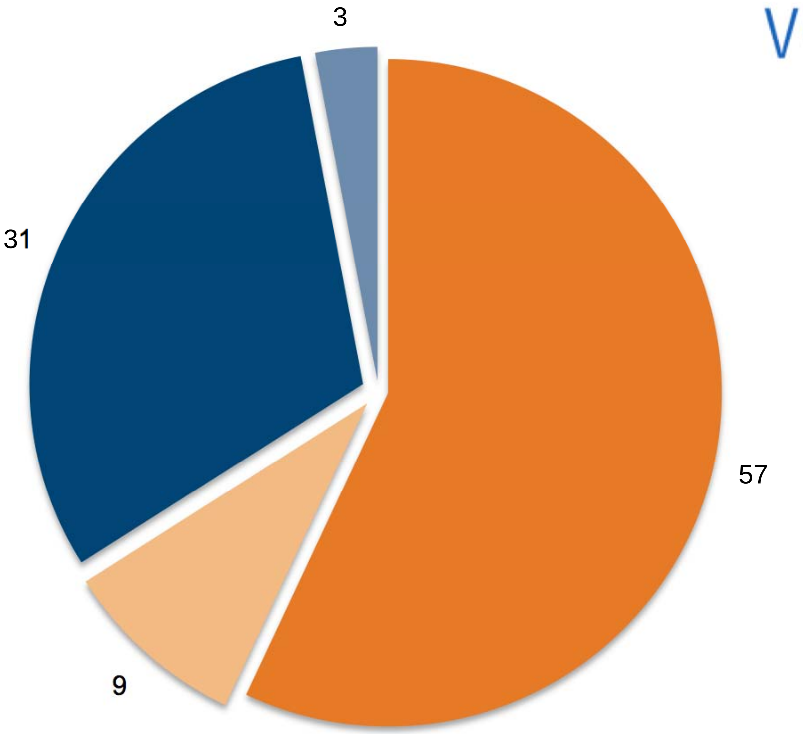
- What forms or **alternative developments** are conceivable?
- What are **potential situations** in the future?

Evaluate projections

- **Probability** of the projection.
- **Impact** of the projection.
- **Security-relevance** of the projection.

The evaluation should be carried out using the Delphi method to collect quantitative and qualitative data; security experts and stakeholder should be surveyed in different panels to **identify divergent perspectives**.

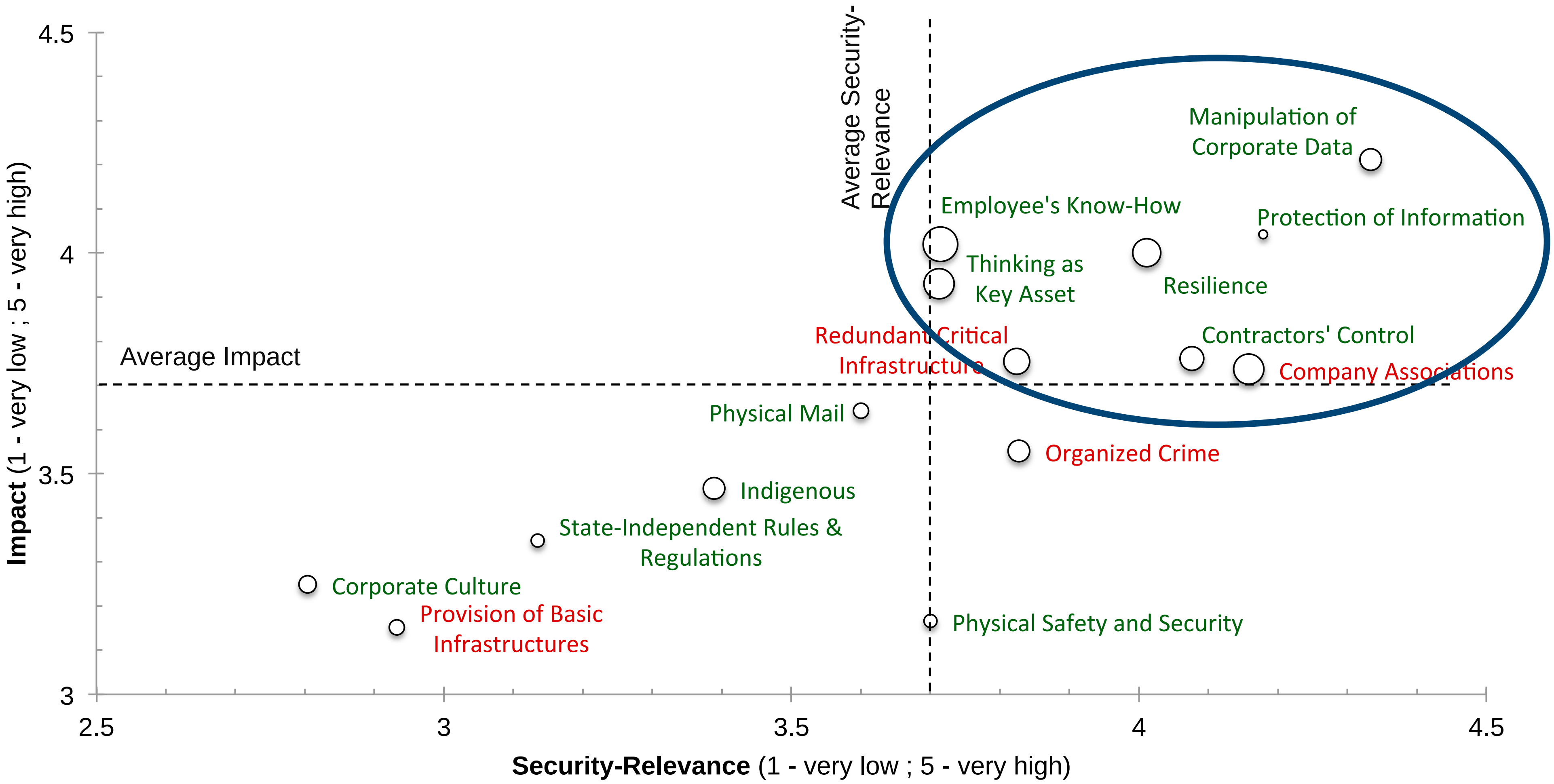
66 Security Experts and 34 Security Stakeholders participated in the Delphi-Panel



■ Security Experts
■ Security Experts (Incomplete)
■ Security Stakeholders
■ Security Stakeholders (Incomplete)

Inspiring Personalities.

Projections regarding the protection of data, information, and know-how bear the highest impact and security-relevance amongst Experts and Stakeholders

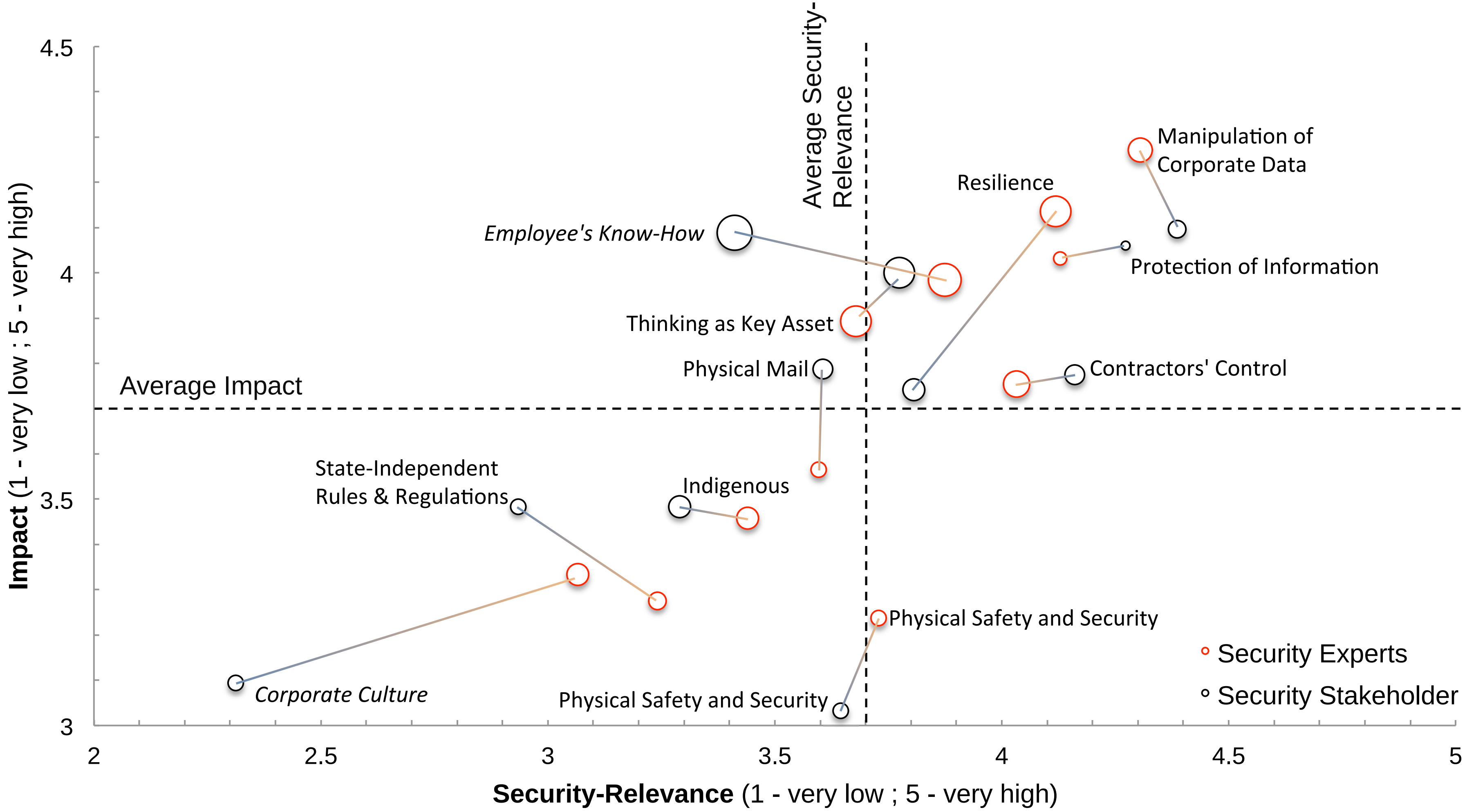


Note. Projections labelled green were evaluated by both security experts and security stakeholders. Projections labelled red were evaluated by security experts only. The size of the bubbles represents the Probability of each projection.

The Delphi-panel argues that the control and protection of data, information, and know-how will continue to be business critical

- A world “without” secrets is considered unlikely. But the terms “protection”, “secrecy”, and “confidentiality” have to be rethought. Finding a good trade-off between security costs and the value of data is becoming important. The focus needs to be more on little but crucial information, which will be increasingly difficult to identify due to decentralised organisations.
- “Confidential” information needs to be protected whilst enabling interactions using “normal communication channels.
- As new work forms will increase, security will have to become an flexible and creative advisor for self-responsible employees. Protection has to happen implicitly, behind the scenes.
- Gaining and retaining the “right” talents and know-how-carriers with experience will be challenge for both, corporations and the corporate security.
- With outsourcing remaining a viable option for management, monitoring physical and logical access to internal information will become ever more important.
- To enable new forms of innovation, adequate information sharing needs to be enabled while protecting internal information at the same time.

Whereas Stakeholders put greater emphasis on projections related to the protection of information, Experts stress projections regarding “governance”



Note. The size of the bubbles represents the Probability of each projection.

Inspiring Personalities.

Besides information protection, security faces further challenges, which are not on stakeholders' top of mind

- Stakeholders consider **resilience** to be implicitly **inherent in a decentralised organisation**, given employee's creativity and flexibility. Security considers resilience to be **part of a centralised business continuity planning and management**. Together with IT and Operations, it could become an essential and renowned part of Security's portfolio.
- **Culture should be used as a lever for security awareness** and security increasingly needs to become an advisor for self-responsible employees.
- States in the developed world will neither give up their law-making authority nor will they fail; but **companies will bear more responsibility and might have greater political influence**.
- **Maintaining (access to) critical infrastructures is a central part of BCM** – and a driver of cost and complexity for Security. In times of major disruption, companies should not rely on state's support.
- A rise of **organized crime** is considered uncertain since its consequences would be born by society, too.
- Also the **benefits of companies being considered indigenous** are considered uncertain since local unrest will always target the perceived rich.

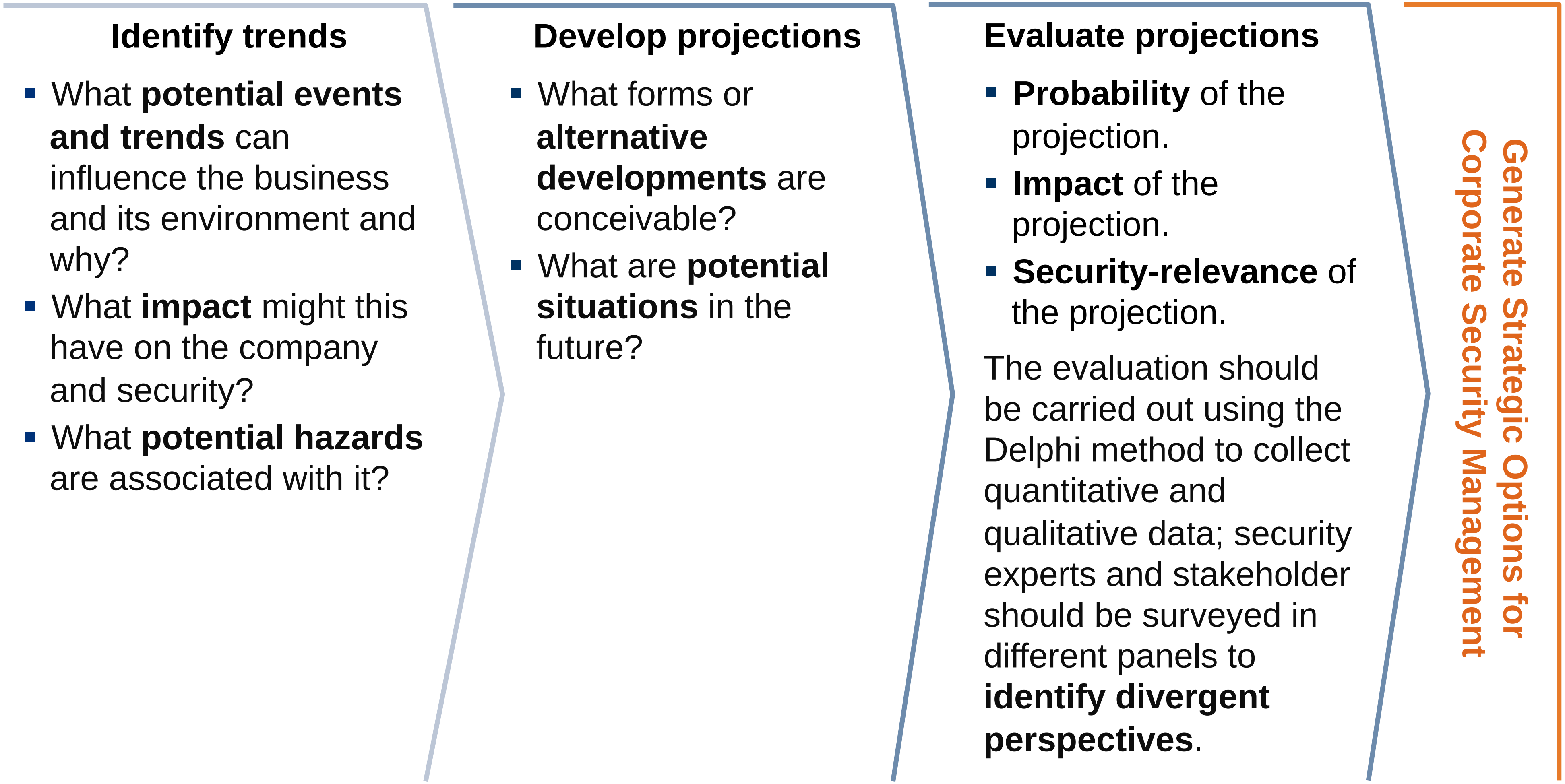
Only few significant differences between Expert and Stakeholder* as well as between the participating companies'** evaluations of projections were revealed

- Only **few significant differences** in perceptions between Security Experts and Security Stakeholders were revealed.
  - Regarding "*Resilience*", Experts considers BCP/BCM potentially central in Security's portfolio. Stakeholders rather belief in the flexibility and creativity of the workforce to encounter disruptions; besides, disruptions cannot be too devastating.
  - Experts see in "*Corporate Culture*" a vehicle to increase security awareness – Stakeholders not. Common to both: Corporate Culture will have to balance the diversity of cultures, thereby, promoting corporate culture.
- Stakeholders evaluate projections related to the **protection of information** ("Thinking as Key Asset", "Employee's Know-How", "Physical Mail", "Contractors Control") generally higher than Experts.
- Experts evaluate projections related to "**governance**" (e.g., "Resilience", "Corporate Culture", "Physical Safety and Security") generally higher than Stakeholders.
- The **qualitative arguments highlight different perspectives** on projections and issues, but, more often than not, indicate a similar understanding.
- Between the companies' Experts participating in the Delphi, only few significant differences in evaluating the projections exist. In most cases these regard the security-relevance of a projection (4) followed by impact (2) and probability (2).

* t-test and z-test for two independent samples / Two-tailed test, 95% confidence interval
** Kruskal-Wallis test, 95% confidence interval

Corporate Security 2030: Research approach

4 – Generate options for Corporate Security Management



Identify trends

- What **potential events and trends** can influence the business and its environment and why?
- What **impact** might this have on the company and security?
- What **potential hazards** are associated with it?

Develop projections

- What forms or **alternative developments** are conceivable?
- What are **potential situations** in the future?

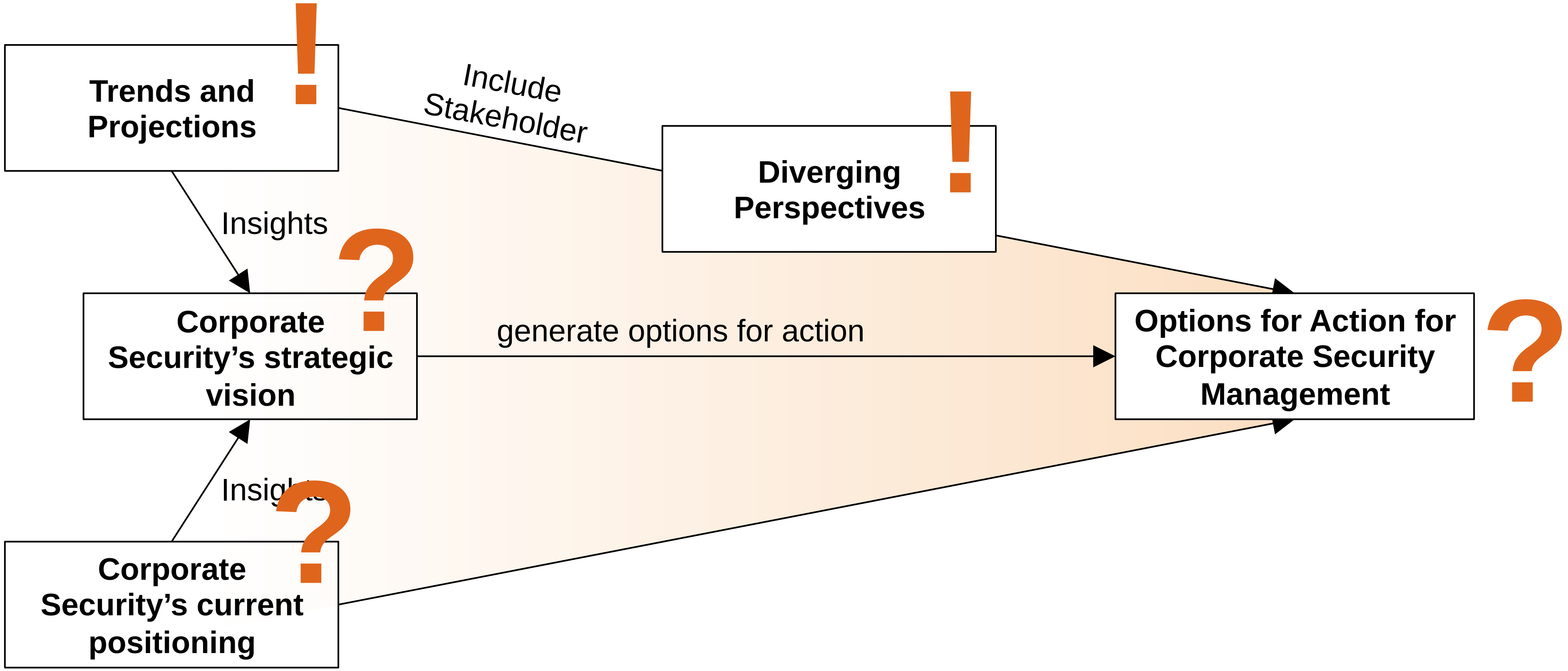
Evaluate projections

- **Probability** of the projection.
- **Impact** of the projection.
- **Security-relevance** of the projection.

The evaluation should be carried out using the Delphi method to collect quantitative and qualitative data; security experts and stakeholder should be surveyed in different panels to **identify divergent perspectives**.

Generate Strategic Options for Corporate Security Management

To generate options for Corporate Security Management, not only insights from the study, but its strategic vision and its current positioning have to be taken into account


Trends and Projections
!
Include Stakeholder
Diverging Perspectives
!
Insights
?
Corporate Security's strategic vision
generate options for action
Options for Action for Corporate Security Management
?
Insights
?
Corporate Security's current positioning

Wack, P. (1985). Scenarios: Shooting the rapids. *Harvard Business Review*, *63*(6), 139–150.

Hot Topics

Building upon the experience and know-how gained during the study, three hot topics could be investigated in follow-up projects

The Future of Information Security

- Data, information, know-how and experience are and will remain to be the key of success for any business.
- But protecting corporate information is a fragmented task: Data is prone to IT-security breaches; Public Relations are a source for business intelligence; and employees are vulnerable to social engineering, among others.
- By investigating trends and projections in information security from a holistic perspective, new insights and perspectives on security a company's most important asset – information – can be gained.
- Incorporating not only Security Experts, but IT Experts and Management, an encompassing picture on the future of information security can be developed.

Security in Future Working Environments

- Interconnected production methods; disperse working locations; customers as value adding partners; and open innovation are only a few trends that will change the working environment in the future.
- Security will have to strike a balance between providing protection and permitting individualisation and connectivity in increasingly complex and scattered organisations.
- By developing robust scenarios for future working environments, security-relevant challenges and opportunities can be identified and sensitive, work related security issues deduced.
- By embracing multiple perspectives and opinions, an action-driven checklist for an anticipatory strategic , R&D, HR, and security management can be developed.

Resilience – Anticipating future disruptions

- Resilience implies not only being prepared for but also being able to cope with disruptions. Although the creativity and flexibility of people is a major driver of resilience, sound concepts on how to adapt, to change, and to react quickly to major disruptions will become increasingly important in times of global uncertainties.
- In cooperation with IT and Operations, Security will have to develop robust BCM plans – especially regarding critical infrastructures – balancing risks, costs and business opportunities.
- Having developed robust and open-minded scenarios, back-casting enables the development of future-oriented early-warning indicators and helps management to discern what is likely to come.

Thank you for your attention!

“ If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

(The art of war, III, 18)

Contact

Prof. Dr. Christoph Georgi
Juniorprofessor für Management,
insb. Security & Innovation

Straschеg Institut for Innovation
and Entrepreneurship (SIIE)
EBS Universität für Wirtschaft und Recht
EBS Business School
Rheingaustrasse 1
65375 Oestrich-Winkel
phone: +49 611 7102 2067
christoph.georgi@ebs.edu
www.ebs.edu/siie

Klaus Burmeister
Managing Partner

Z_punkt GmbH
The Foresight Company
Anna-Schneider-Steig 2
50678 Köln
phone: +49 211 355 534 10
burmeister@z-punkt.de
www.z-punkt.de

Inspiring Personalities.

Appendix A

The 11+4 Projections

Projections

11 projections were evaluated by both Security Experts and Corporate Security's Stakeholders

Employee's Know-How	Today, the availability of skilled workers and qualified staff is subject to many discussions labelled the "War for Talents" or "Brain Drain", amongst others.	In 2030, employees with know-how and experience are the most valuable and most important assets that companies try to gain and retain.
Protection of Information	Today, company internal information is considered deserving protection although access to it is neither limited to employees only nor can leakages be prevented.	In 2030, the protection of company internal information and secrets is considered useless.
Physical Mail	Today, foremost digital communication channels such as IP-telephony, e-mail and social media are used to coordinate company's global activities.	In 2030, physical mail and face-to-face communication have once again advanced to be the prime channel for confidential communication.
Corporate Culture	Today, corporate culture characterises people not only in business but also in private life.	In 2030, corporate culture – instead of one's origin – defines one's identity, marginalising cultural differences in a multicultural world.

Projections

11 projections were evaluated by both Security Experts and Corporate Security's Stakeholders

Physical Safety and Security	Today, laws require company's to provide for employees' safety and security at work. Yet, new forms of work (e.g., home office or telecommuting) increasingly blur the definition of "workplace".	In 2030, employees' are required to provide for their own physical safety and security.
State-Independent Rules & Regulations	Today, associations represent their members' interest and lobby for favourable national and transnational policy making.	In 2030, companies have compiled state-independent rules and regulations that are tolerated by local authorities across the globe.
Resilience	Today, business continuity planning is on the fringes of management tasks related to risk and IT.	In 2030, only companies that have strengthened their ability to withstand severe disruptions (i.e. their resilience) within their management and workforce are still in operations.
Contractors' Control	Today, companies depend on contractors such as service companies and manufacturers to carry out specific activities thereby granting them limited access to processes, information, and know-how.	In 2030, due to the high dependence on contractors they have gained full access and control over internal processes, information, and know-how.

Projections

11 projections were evaluated by both Security Experts and Corporate Security's Stakeholders

Manipulation of Corporate Data	Today, cyber attacks not only targeting data but industrial machinery is possible as was proven by Stuxnet's ability to destroy Iranian uranium enrichment facilities.	In 2030, the manipulation of corporate data (cyber sabotage) has caused sever production downtime / breakdowns decreasing output in average by 40% annually.
Indigenous	Today, companies' are engaged in corporate social responsibility and local community development project especially in undeveloped countries.	In 2030, only companies that are considered to be integral part of the respective society by locals due to their long lasting proactive support of local development activities are not imperilled by social unrests.
Thinking as Key Asset	Today, ever-growing amounts of data and information is being stored, made available and analysed.	In 2030, data and information is available by and large – hence, individual thinking is a company's key asset and requires careful and sensitive handling.

Projections

+4 projections were evaluated by the Security Experts only

Provision of Basic Infrastructures	Today, in failing states and underdeveloped regions companies provide their local employees and expats with water, food, and health care.	In 2030, even in the developed world, companies have taken on states' obligations to provide their employees and relatives with basic infrastructures such as water, food, and health care for their employees and relatives even in the developed world.
Organized Crime	Today, organized crime is primarily associated with human trafficking, drugs, and money laundering; its involvement in economic activities such as waste management is largely unnoticed.	In 2030, organized crime has taken over major target markets of companies that were hindered to operate profitable in the respective market.
Redundant Critical Infrastructure	Today, operators of critical infrastructure such as utilities can hardly maintain redundant infrastructures since they are subject to market forces.	In 2030, only companies that have secured themselves access to or maintained their own redundant critical infrastructures remain in business.
Company Associations	Today, organised crime invests heavily in capabilities for infiltrating IT infrastructures and conducting cyber attacks, which are readily available on profitable black markets well in advance of security vulnerabilities being known by experts.	In 2030, only associations of like-minded companies are able to prevail the spiralling arms race between companies and organised cyber crime.