VICCON

CONSULTING

Next Generation Security Management

An innovative approach to the further development of safety management for the 4th Industrial Revolution

A guide for CDO, CIO and CISO

IMPRINT

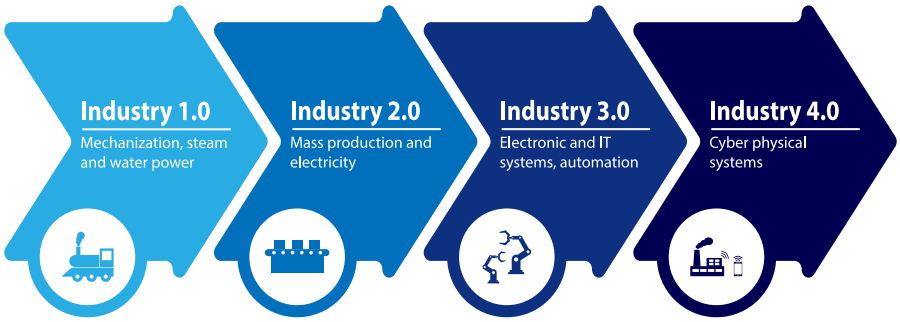
Brochure: Next Generation Security Management - An innovative approach to the further development of safety management for the 4th Industrial Revolution

4. INDUSTRIAL REVOLUTION AND DIGITAL TRANSFORMATION

After industry has been largely automated in recent decades, networking and the Internet have since 2000 created the conditions for reaching a further evolutionary stage in industrialization, the 4th Industrial Revolution (4IR), also known as Industry 4.0.

An essential feature of this level is a very high degree of automation in the production or use as well as the communication of the technical elements involved in the product, which independently inform each other about their conditions and activities and, if necessary, make autonomous decisions. In the future, this will increasingly happen on the basis of artificial intelligence and include more and more services from third-party providers as well as the networked supply chain. New services refine or individualize the digital product. Elements of the networked digital product are not only the connection to the Internet, the operation with an app, but also, for example, the collection of data for purposes of usage analysis or predictive maintenance. Thus, these digital functions can also have a security relevance in the sense of functional safety. Cyber Security becomes part of Functional Safety. Thus, cyber security, data protection and information security become central elements of the 4th Industrial Revolution. This requires a well-thought-out digitalization strategy of every company, on the one hand in the value chain itself, on the other hand in a common control of these topics, the security management.

Foreseeable and unpredictable technological developments will fundamentally transform many industries. In order to manage these changes, new frameworks or comprehensive cooperation will not suffice in the future. Adapted working methods and processes as well as new models for knowledge and competence transfer will also be required, which fit the fast pace of the market and the workforce.



CYBER NORMS AND LIABILITY

In order to be able to understand the situation to which one is exposed as a company, one must be aware that there is currently no internationally binding framework for states to behave in cyberspace. While most states have recognized cyberspace as a military domain, the UN is not yet in a position to agree on "responsible state behaviour" in cyberspace and to adopt cyber norms. Cyber-attacks are therefore not prohibited in all states or are covered by their legal systems. Thus, one's own liability cannot be passed on to the perpetrator. A prosecution for damages is therefore not always possible. In many countries, cyber defence is also organised only for the official sector, but not for the private sector. Accordingly, cyber threat information is shared only very cautiously with the economy at the state level. The protective principle of the state for the defence against military or state attacks on the economy is not effective in cyberspace. Threat intelligence and defensive measures and prosecution of perpetrators must therefore be handled by companies themselves, even though the attribution of cyber-attacks to their origin can hardly be solved by companies and is usually politically sensitive. Corresponding competence building in these fields for the economy is only insufficiently mapped at the level of state training and further education opportunities. As a company, one must therefore prepare oneself for a professional attacker. Products and services that are sufficiently attractive for attackers must be adequately protected by the company, especially if they have a safety relevance. In the case of networked systems and services with third parties, risk assessment and maintaining a uniform level of security present companies with major challenges.

A further aspect, in addition to the data protection laws of the individual states or regions, is the handling of data that states require to be processed and stored in the country. In the case of key economic technologies, this can go so far as that the country requires to integrate national encryption or control technology into its corporate networks. As far as data protection is concerned, there is the approach, which is mostly advocated in the West, that personal data belong to the person concerned, while in other parts of the world data is seen as part of the Internet infrastructure and thus assigned to the sphere

of influence of the state. In any case, one can easily see that data and cyberspace are increasingly subject to political influence and more and more under control and regulation. Prohibitions on the use of encrypted communication or algorithms by companies supplement this, as do patents on software or restrictions in the supply chain. This may affect the use of certain cloud services from other third-party services. Therefore, when considering digital products, such aspects must be taken into account and considered holistically.

In any case, one can see that data and cyberspace are increasingly subject to political influence.

DIGITAL TRUST AND NETWORKED TRADING

Cyber-based sabotage, espionage and crime are constantly watching and the attackers are becoming more and more experienced. The more dependent your product is on cyberspace, the more important it is to consider all relevant aspects in a consistent approach. Since cyber-attacks presuppose existing vulnerabilities that cannot be avoided with software-based systems of a certain complexity, consideration begins here. If digital preliminary products are purchased and used, a conscious decision concerning the risks is necessary. Is the supplier or manufacturer trustworthy? Does the component or service offer sufficient security?

These questions are not easy to answer, but the associated risks can be controlled within the company using a suitable risk methodology. Internationally recognized certifications or references also offer digital trust. The traceability of such corporate decisions and the standards chosen for them will become increasingly important in the future, be it for product liability, insurance or legal investigations in case of damage. Security management can help to avoid organisational liability. This can occur if managers make the wrong decisions in corporate actions that cause damage to third parties. Another way to securely integrate digital products into the value chain is to take a holistic approach that includes business IT, IT in the conceptual phase, in the production phase and in the operation and maintenance phase of the product.

However, it is not enough today to organise this separately in departments so to say in silos. Availability, confidentiality and integrity run along work processes. If data communication and data processing exist across all areas, e.g. in PLM systems, these must be secured across all process steps. If CAD/CAM data flows through the business processes and creates prototypes, managers must protect them in the business processes if necessary. If software is developed for a product with business IT and goes through different phases of the manufacturing and maintenance process, the safety and quality requirements for the product must be considered right from the start in the business IT. In terms of product lifecycle phases, a company may need to consider taking a product back from the customer at the end of its lifecycle in order to protect the inherent digital know-how. Agile working methods are popular, but they push traditional know-how protection methods to their limits. This can only be achieved with a complementary security culture and by taking the human factor into account.

Availability, confidentiality and integrity run along work processes.

SECURITY STRATEGY

Trends and topics such as resilience, networked society and new work must be considered in future considerations.

While security management is usually subject to the requirements of the organization and integrated into the existing management, performance and support processes, cyber security and IT security are subject to other requirements.

The approach of raising cyber security or IT security to the same qualitative level as in product creation appears necessary and promising. This means locating this discipline on the level of engineering principles, methods and procedures and no longer accepting that the security of software and IT depends on the random level of knowledge of individual employees. This requires appropriate control over the entire company. This can happen, for example, through the cooperation of the Chief Digital Officer (CDO), the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO).

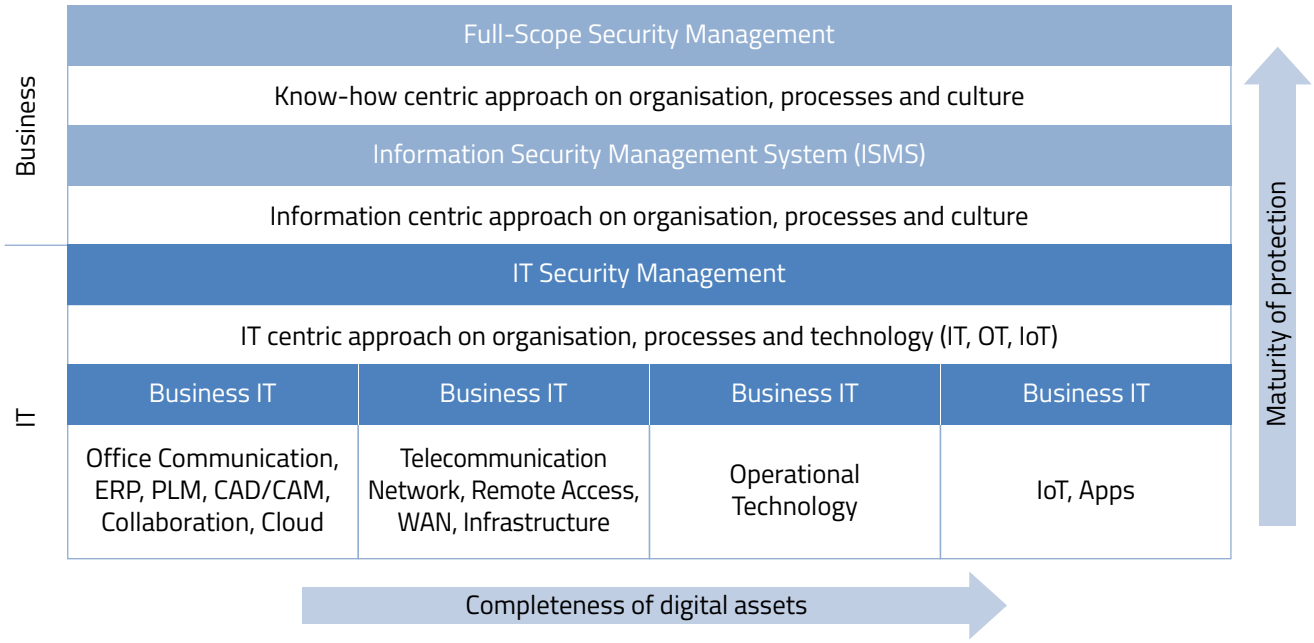
While the CDO's contribution to security in digital transformation consists in particular in explaining to the security authorities what the security requirements are from the point of view of the company and its customers, the CISO's task is to organise cross-company information security in such a way that the CDO's requirements are guaranteed over the lifetime of the products and services. The CIO's role is to integrate the CISO's information security standards into the IT projects and services required for digital products. Ideally, all three roles should have corresponding strategies that are interlinked or have a common strategy.

Trends and topics such as resilience, networked society and new work must be incorporated into future considerations. VICCON processes such requirements in a security strategy in which concrete measures for the future work of the security departments and the entire company are derived with a methodical approach.

NEXT GENERATION SECURITY MANAGEMENT

The creativity of attackers in cyberspace is inexhaustible. Companies only have a chance if information security functions in an orderly manner, for example if it is organised via a security management system (SMS) that adequately maps topics such as know-how protection, information protection and cyber security or IT security and includes them in the company's risk assessment. The company management is informed about the security risks and can make conscious decisions about them.

VICCON Next Generation Security Management not only comprises a holistic approach in the sense of full scope security management, with all the aspects mentioned, but also supplements this with a proven and constantly further developed process model for security management, which can be brought to certification depending on its characteristics. This process model is suitable for adapting the aforementioned aspects to the needs of the company and rolling them out in the international subsidiaries, thus centrally controlling security. VICCON advises on the establishment or restructuring of a security management system and provides all the necessary services and instruments, both nationally and internationally.



ADVICE - DIALOG - KNOWLEDGE TRANSFER - IMPLEMENT - EDUCATE

For about 20 years, VICCON has supported organizations in understanding security-relevant developments, building up the necessary know-how and processes for them, thus allowing them to control them securely.

With you and in dialogue with all company levels, VICCON develops ideas and seeks a suitable orientation for the security policy in the light of the different requirements.

VICCON develops strategies for secure and resilient organizations, follows the digital transformation and advises on the implementation of these strategies in the form of Next Generation Security Management.

VICCON pursues the goal of strategically anchoring security in the company according to management and business policy. Particular emphasis is placed on information security management, the management of cyber risks as well as prototype and know-how protection.

CONTACT

For further information please contact us:

VICCON GmbH

Ottostrasse 1
76275 Ettlingen
Germany

Phone: +49 7243 719734
Fax: +49 7243 719704

E-mail: info@viccon.com
www.viccon.com

VICCON

CONSULTING