Whitepaper —
EFFECTIVE PROTECTION OF CRITICAL INFRASTRUCTURE

DEKRA

Increasing digital networking simultaneously creates both opportunity and risk. While digitalization has spurred entirely new industries, existing companies are now able to reach customers and business partners around the world at any time of the day. In addition to all the possibilities, however, there are a number of threats challenging companies, especially those providing critical infrastructure.

In 2017, the "WannaCry" malware caused a worldwide stir and affected numerous hospitals of the National Health Service in the United Kingdom. More than 26 million records with sensitive personal data were compromised in this large-scale cyberattack, and financial losses totalled a whopping £92 million (US$113m).

Failures affecting critical infrastructure, such as utilities, hospitals, telecommunications services, banks, and airports can pose major problems on a national or global scale. The risk of failure, disruption, or manipulation is high and may result in sustained supply shortages, significant public safety issues, or other serious consequences for the community.

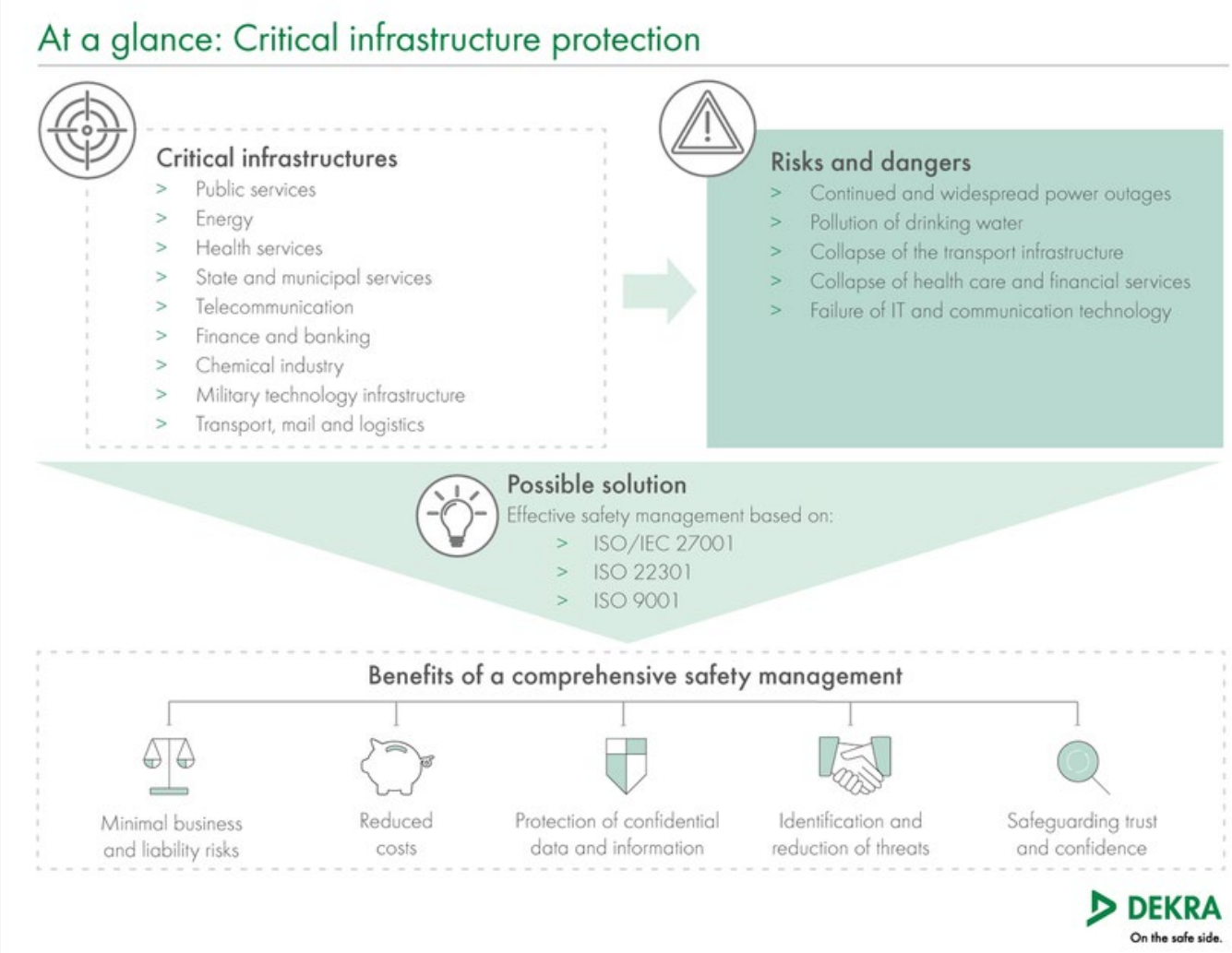
A legally compliant, technically secure, and economically efficient IT security architecture is therefore indispensable. Certification to the internationally recognized DIN EN ISO/IEC 27001 information security standard can help companies fortify their critical infrastructure.

Developing and documenting appropriate IT processes can help to map information security needs to the appropriate risk situations. In order to adopt effective security strategies, responsible company officials must understand their particular internal and external infrastructure requirements. It is their knowledge of critical IT core components, services, and processes that will enable them to assess, control, and protect these elements to avoid potential liability claims.

As with the globally applied ISO 9001:2015 quality management standard, information security management systems (ISMS) according to the DIN EN ISO/IEC 27001 standard are based on the so-called high-level structure (HLS).

Reliable information security concepts are based on fundamental documents of quality management describing technical and organizational measures, as well as assessed protection classes.

The responsibility for reliable and secure IT operations lies with company management. Corporate leaders must pay special attention to the effectiveness of IT security architectures, as well as the ongoing implementation of improvement measures to maintain reliable security structures responsive to cyber threats of all kinds. In addition, corporate management should be prepared for any eventualities caused by cyber-attacks by implementing a business continuity management (BCM) according to ISO 22301. This ensures that the central operational functions of the organization are maintained even after an emergency and that business activities can quickly resume.



DEKRA Audits
Certification and training in ISO 9001, ISO 14001, ISO 27001, ISO 50001, AS9100, and many more!

1120 Welsh Rd.,Suite 210, North Wales, PA 19454

1-800-768-5362
sales.us@dekra.com
www.dekra.us/audits