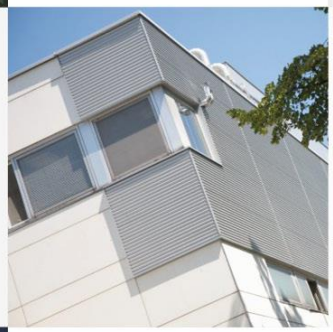
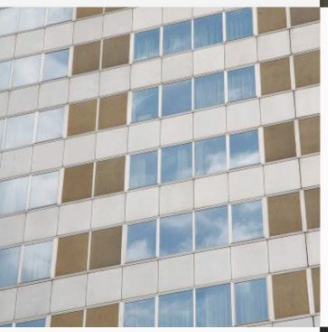
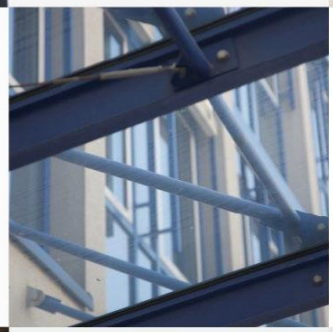
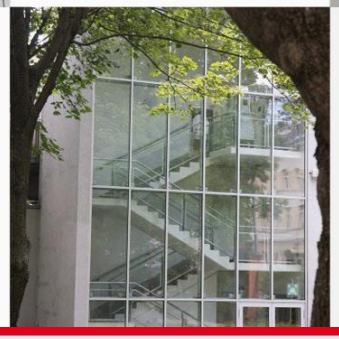


“The challenges of the NIS directive”

from the viewpoint of the Vienna Hospital Association”

Fotos: KAV

Cybersecurity Strategy – Essential Points

- The norms, principles and values that the City of Vienna and the the Vienna Hospital Association uphold offline, should also apply online

- Cyberspace must be correctly protected

  ✓ The City of Vienna has a significant role to play in ensuring a safe cyberspace

  ✓ The City of Vienna and the Vienna Hospital Association augment this situation by ensuring respect of fundamental rights online

The Crux of Cyber Resilience

- Digital technology touches virtually every aspect of daily life today:
  - ✓ Social interaction, political engagement or economic decision-making and also healthcare activity

- Digital connectivity impinges on all of these, and the dependence on this connectivity is growing swiftly

- It is necessary to develop a common set of expectations to address systemic risks, and to define not only the roles but also the responsibilities of all participants in the cyber ecosystem

The Crux of Cyber Resilience (cont.)

- The **collective ability to manage cyber risks** in this shared digital environment is fundamental.
- Information security relates to a core aspect of modern life

TRUST in the

- strategic infrastructure that we need
- people who work with it every day
- **E-Health applications**, we work with
- suppliers of **E-Health products** and medical devices

Uncertain information can destroy this trust!

"It's about nothing less than the question of how an instrument can be mutually created in the **work style** of the **health** and **social care community** to be safe, reliable, efficient and trustworthy"

It's about lifelines in a modern society

Perspectives of ICT in Hospitals and Healthcare

- Altered structures in healthcare and integrated care models require ICT for their implementation

- Healthcare needs to became more:
  - ✓ **patient-centered** and **user-oriented**
  - ✓ **knowledge-based**
  - ✓ **process-oriented** and
  - ✓ **output-oriented**
- Increasing globalization and networking of healthcare processes also increase cyber vulnerability and increase the importance of the above aspects

Strategic Objectives

- To strengthen cyber resilience
- To develop a cyber defence policy and related capabilities in accordance with Austrian national security and defence policy
- To develop technological resources for cybersecurity
- To reduce cybercrime by working together with the National Association of Computer Emergency Response Teams (CERT-Verbund: HealthCERT, GovCERT, MilCERT, WienCERT, …)

Achieving Cyber Resilience

- Requires the establishment of a cybersecurity culture to enhance business opportunities and competitiveness
- Requires the exchange of information between, and the reporting of significant incidents to, members of the **National Association of CERTs / CSIRTs** and other regulatory bodies
- Requires the improvement and expansion of cybersecurity exercises, in combination with civil defence exercises, as carried out by the Vienna Hospital Association and the City of Vienna

Achieving Cyber Resilience (cont. 1)

- The strategy should aim to increase cooperation and transparency relating to cybersecurity in ICT activity.
- A high degree of cybersecurity can only be guaranteed if all contribute something to the value chain for cybersecurity.
- Cooperation with relevant stakeholders in the development of technical guidelines to identify emerging trends relating to cybersecurity, and security in general, is necessary.

Achieving Cyber Resilience (cont. 2)

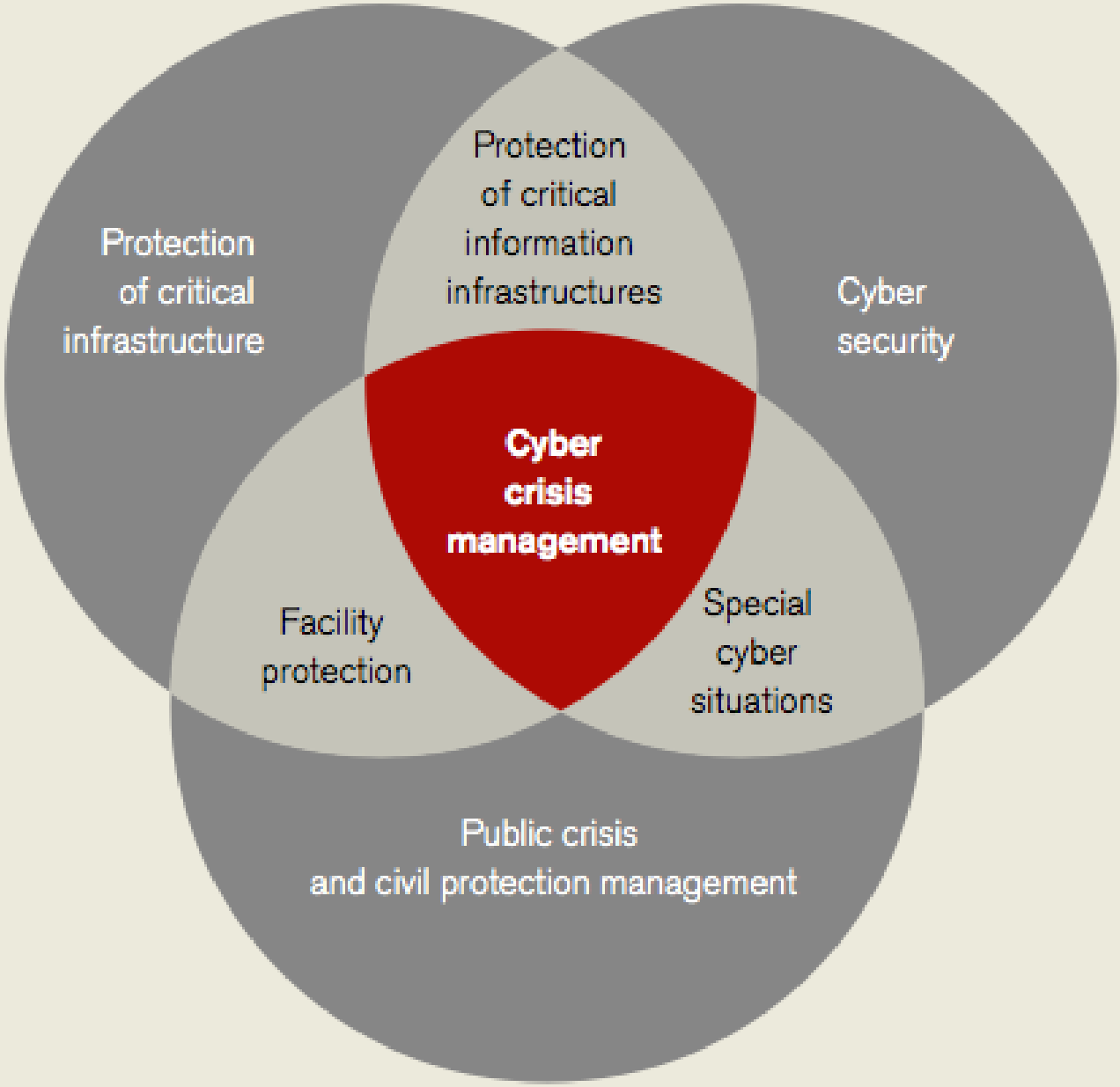
- A public private partnership structure for coordination at operational level involving the business and research sectors should be created
- It should be designed as an operational executive body for overall cyber crisis and civil defence crisis management
- A periodic and incident-related **Cybersecurity Overview** of the threat situation in cyber space should be prepared and published

Cyber Crisis Management as a part of Civil Defence Crisis Management

- Austria's **Cyber Crisis Management** involves state, provincial and local authority administrations, and operators of critical infrastructure. Vienna's **Civil and Cyber Crisis Management** is a part of this.

- It is modelled on the Governmental Crisis and Civil Protection Management architecture (SKKM)

- Crisis management and continuity plans are prepared and updated regularly on the basis of risk analyses for sector-specific and cross-sectoral cyber threats

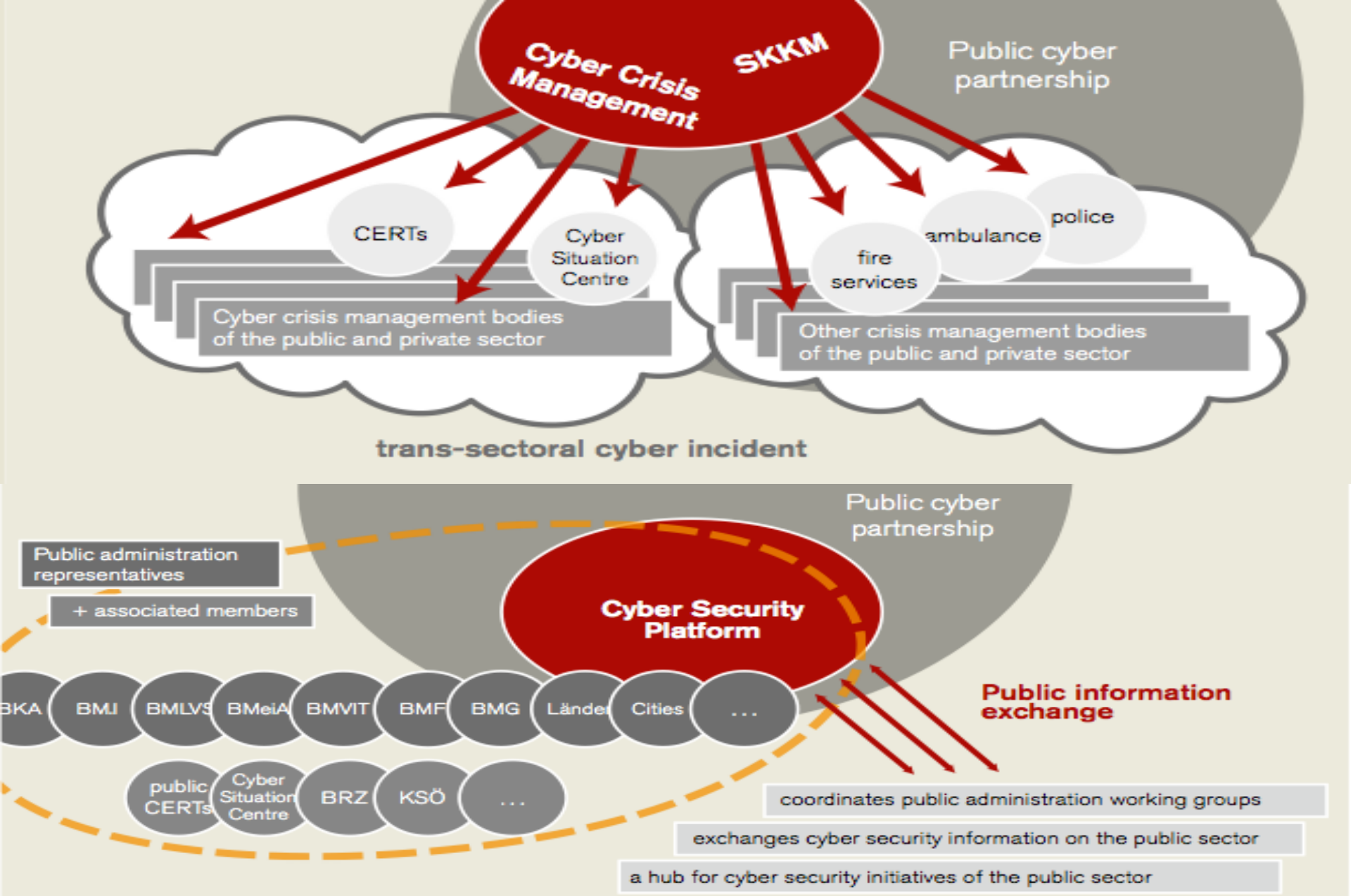

Protection of critical infrastructure
Protection of critical information infrastructures
Cyber security
Cyber crisis management
Facility protection
Special cyber situations
Public crisis and civil protection management

Establishing a Regulatory Framework

- Institutions can take all the actions they want on their own, but if there is no law-enforcement mechanism to pursue and prosecute perpetrators, then their actions are meaningless.
- A balance between incentives and sanctions must be set to ensure the performance of non-state actors
- In order to guarantee cybersecurity in Austria, it is necessary to establish an additional legal framework, regulatory measures and self-commitment (code of conduct)

Establishing a Regulatory Framework (cont.)

- The following points are important for the additional legal framework:
  - ✓ Information exchange between authorities and non-state actors
  - ✓ An obligation of the state, private industry, and research sectors to report incidents to the cyber security centre
  - ✓ A duty to adopt protection measures
  - ✓ The security of the private industry and the research sectors' supply chains is also important


Cyber Crisis Management
SKKM
Public cyber partnership
CERTs
Cyber Situation Centre
Cyber crisis management bodies of the public and private sector
ambulance
police
fire services
Other crisis management bodies of the public and private sector
trans-sectoral cyber incident
Public cyber partnership
Public administration representatives
+ associated members
Cyber Security Platform
BKA
BMI
BMLVS
BMeiA
BMVIT
BMF
BMG
Länder
Cities
...
public CERTs
Cyber Situation Centre
BRZ
KSÖ
...
Public information exchange
coordinates public administration working groups
exchanges cyber security information on the public sector
a hub for cyber security initiatives of the public sector

Cooperation between Stakeholders

- The responsibility to use digital technology in a prudent way rests with each individual organizational unit.
- But only broad cooperation between all sectors and regular mutual exchange of information will make the use of ICT transparent and safe.

Support for Small and Medium Enterprises

- Priority programmes on cybersecurity will be launched to raise awareness amongst small and medium enterprises (SMEs) concerning cybersecurity
- Sector-specific information platforms such as the "Austrian Trust Circles" should help to develop cyber risk management plans for SMEs
- These risk management plans should be coordinated with governmental crisis and continuity management plans

Protection of Critical Infrastructure

- Today almost all sectors of infrastructure increasingly depend on specialised ICT systems
- It is therefore a top priority to improve the resilience of these ICT systems against cyber threats
- Under the "Austrian Programme for Critical Infrastructure Protection", enterprises operating critical infrastructure systems are encouraged to introduce comprehensive security architectures

Protection of Critical Infrastructure (cont. 1)

- The enterprises operating critical infrastructure systems should be involved in all processes of national and also regional crisis management

- Existing arrangements for the protection of critical infrastructure and the national and regional crisis and civil protection management should be reviewed on an ongoing basis to ensure that they continue to meet new cyber challenges and the protection plans should be modified if required

Protection of Critical Infrastructure (cont. 2)

- Enterprises involved in critical infrastructure should have a duty to report severe cyber incidents
- Crisis communication should be further developed and intensified
- Enterprises involved in critical infrastructure should set up a default comprehensive security, risk and crisis management architecture

Awareness Raising and Training

- By sensitising all target groups, the necessary awareness of, personal interest in, and attention to cybersecurity will be increased
- These awareness-raising measures will help to create understanding for the need to ensure cybersecurity in Austria

Awareness Raising and Training (cont.)

- A meaningful and adequate ICT competence level should be ensured by expanding training in the field of cyber security and media competence in schools and other educational facilities as well as by developing national cyber security competence in the apprenticeship training system

- Awareness-raising initiatives should be developed, coordinated and implemented on the basis of a common approach incorporating existing programmes

Strengthening a Cybersecurity Culture

- In this context it is important to examine cybersecurity from different perspectives, to highlight relevant dangers, to draw attention to possible effects and damage as well as to make recommendations for additional security measures
- To ensure cybersecurity, technical expertise is necessary, which must be based on state-of-the-art research and development results
- Cybersecurity must be among our key research priorities

Effective Collaboration on Cybersecurity

- The free exercise of all human rights must be guaranteed in virtual space, and particularly the right to freedom of expression, and information must not be restricted in cyber space
- This is the position Austria should adopt in international forums
- Hence, Austria should participate actively in developing and establishing a transnational code of governance in cyber space, which will include measures to build confidence and security

Thank you for your attention

Franz Hoheiser-Pförtner

Chief Information Security Officer

Certified Information Systems
Security Professional (CISSP)

Vienna Hospital Association

phone +43 1 40409 66017

e-mail: franz.hoheiser-pfoertner@wienkav.at