Cybersecurity Checklists for Holiday Season Readiness and Emergency Response

Preparing for a Cyberattack – Checklist for a Secure Summer

The well-deserved holiday is approaching – but cyberattacks are at their peak, especially during holiday season.

Is your company adequately protected during this time?

Good **preparation** is essential!

"Schoenherr takes a tactical and client-centric approach to challenges. It has creativity and the ability to think outside the box."

Chambers Europe

"Highly professional services. Always available as a trusted legal partner."

Legal 500

Let's pack some tips and guidance into your (digital) suitcase together:

- ☐ Are **roles and responsibilities clearly** defined in case of an emergency – and have holiday absences been coordinated?
- ☐ Is your **staff** – even in the absence of management – **aware** of common cyber and social engineering attacks, prepared to respond appropriately, **familiar with reporting obligations** and informed about **relevant deadlines**?
- ☐ Are **emergency contacts** (e.g. incident responders, IT forensics, legal advisors) readily accessible?
- ☐ Is a suitable (cyber) **insurance** policy in place and are all obligations arising from the policy known to the responsible parties?
- ☐ Have **holiday cover arrangements** been made and is **on-call availability** during **weekends** and **public holidays** clearly regulated? (Important: Reporting deadlines for notifiable incidents apply even during holidays, weekends and public holidays – for example, 15 August in Austria.)
- ☐ Are all security-relevant systems up to date? (Are the **latest updates** installed? Are firewalls correctly configured? Are backups complete, securely stored and current?)
- ☐ And last but not least – **the most important question:** Has this checklist been **printed** and **placed in a clearly visible** spot in the office?

Cyber Emergency – Checklist in the Event of a Cyberattack or Cyber Incident

From the **very first suspicion** of a cyberattack or incident, the following applies:

Immediate notification of the relevant stakeholders:

- IT department
- Chief Information Security Officer (CISO)
- Legal department
- Data Protection Officer
- Legal counsel
- Incident Response Team (if applicable)

Emergency Contact

24/7 Emergency email:
cyberincident@schoenherr.eu

Rapid support available for:

Legal assessment of the situation; handling of reporting obligations; coordination with incident responders and IT forensics experts; evaluation of potential recourse claims; assistance with correspondence involving authorities

- ☐ **Fact-finding:** What exactly has happened? Is the attack or incident still ongoing, or has it been contained?
- ☐ **Documentation:** Careful recording of the incident and – where possible – collection of forensically usable evidence, even during ongoing recovery and repair efforts.
- ☐ **Assessment of the situation:** Evaluation of the incident regarding scope, severity and potential consequences.
- ☐ **Notify your insurer (if applicable):** Pay attention to notification requirements and contractual obligations and make use of available support where applicable.
- ☐ **Notify authorities:**
  - Compliance with statutory reporting deadlines
  - Data protection authority: within 72 hours at the latest
  - Immediate reporting under the NISG
  - Notification of other authorities (e.g. police), if required
- ☐ **Listed companies:** Pay attention to any additional obligations.
- ☐ **External communication (if necessary):** Ensure strategic and legally sound coordination before informing third parties or the public.
- ☐ **PR measures:** Prepare internal and external communication carefully.
- ☐ **Stay calm:** Deliberate and coordinated action is key!

further information:
www.schoenherr.eu/cybersecurity