TaylorWessing

Hidden danger: Cybersecurity attacks

Protect your business from threats, liabilities, and future risks with an all-in-one legal cybersecurity partner

Hidden Danger
Cybersecurity-Attacks

Cybersecurity is no longer just an IT issue. It is a business-critical priority.

With over 1,600 cyberattacks weekly across Europe - an 86% rise within one year - swift action is essential.

Our holistic approach:
PROTECT, MANAGE, RECOVER

From regulatory compliance to active incident response and future-proofing your organization, Taylor Wessing provides end-to-end support to help you stay ahead of evolving threats.

With a proven combination of cyber, data, IT, and dispute resolution expertise, we help businesses:

- mitigate risks proactively,
- respond effectively during incidents, and
- strengthen resilience for the future.

Also, we have established a network consisting of experienced IT specialists, PR teams, and negotiators to provide a well-rounded response to incidents, ensuring your business is supported on multiple fronts.

TaylorWessing

Our services in detail

1. PROTECT – Minimize risks before they happen

- **Compliance and documentation review:** Ensuring your policies, contracts, and documentation meet e.g. NIS2 and other regulatory requirements.
- **Cybersecurity framework optimization:** Evaluating and enhancing your processes to ensure risk management across your organization.
- **Board advisory:** Advising on liability risks associated with insufficient cybersecurity measures.
- **Vendor and partner contracts:** Reviewing, drafting and negotiating cybersecurity-related provisions in contracts to reduce liability exposure.
- **Insurance review:** Assessing the adequacy of your cyber liability insurance coverage to include critical areas such as regulatory fines, incident response costs, and business interruptions.

TaylorWessing

2. MANAGE – Swift action when every moment counts

- **Immediate legal support:** Representing and negotiating to protect your business's interests during an ongoing incident.
- **Crisis management support:** Supporting to mitigate the impact of scams, blackmail, ransomware, and operational disruptions.
- **Regulatory notification:** Handling reporting requirements and communications with authorities, including breach notifications.
- **Claims management:** Assisting with defending claims against your business and pursuing active claims for recovery of losses caused by third-party negligence.

3. RECOVER – Learn, adapt, and strengthen

- **Lessons learned analysis:** Conducting post-incident reviews to identify weaknesses in your systems, contracts, and processes.
- **Futureproofing:** Implementing recommendations to enhance your security framework and prevent recurrence.
- **Training programs:** Equipping your team with the knowledge to recognize threats and respond effectively.

What our experience teaches us: Lessons learned in cybersecurity response

1. Ransomware attack:

"We supported a client in mitigating a large-scale ransomware attack affecting their operations, ensuring regulatory compliance while recovering critical data. Our rapid response helped them avoid significant fines."

Lessons learned: The sooner an attack is identified and responded to, the less damage it can cause. Having a task force of specialists from areas like insurance, law, forensics, and PR in place in advance is key to saving time and money during a cyberattack. The right team, ready to act, makes all the difference.

2. Executive accountability for cybersecurity failures

"After a significant cyberattack, we discovered that the executive team had failed to implement adequate cybersecurity measures, leaving the company unprepared. We pursued legal action against the executives for not fulfilling their responsibility to protect the organization from cyber risks."

Lessons learned: Cybersecurity readiness is a critical responsibility of the top management. Executives must prepare accordingly.

3. Insurance gap identification:

"Through our insurance review process, we identified a client's cyber liability policy gaps, ensuring comprehensive coverage against regulatory fines andoperational downtime."

Lessons learned: Cyber threats evolve quickly. It is crucial for businesses to regularly review their cyber insurance policies to ensure they are adequately covered.

TaylorWessing

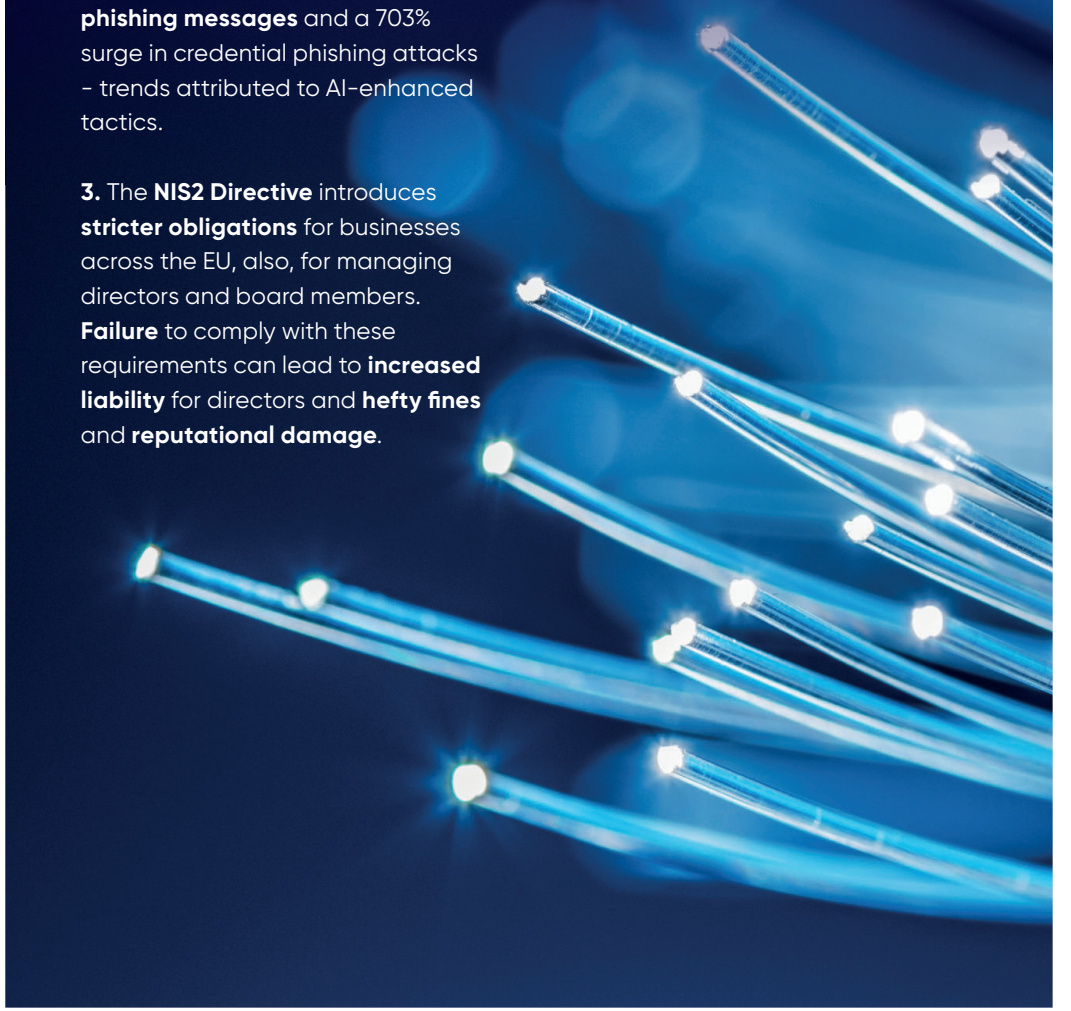
Did you know?

1. In 2024, **cybercrime losses** in Europe reached **€10 billion**, doubling the previous year's figures.

2. Just in the second half of 2024, there was a **202% increase** in **phishing messages** and a 703% surge in credential phishing attacks - trends attributed to AI-enhanced tactics.

3. The **NIS2 Directive** introduces **stricter obligations** for businesses across the EU, also, for managing directors and board members. **Failure** to comply with these requirements can lead to **increased liability** for directors and **hefty fines** and **reputational damage**.

4. Despite the rising threats, **74%** of companies in the EU reported **not providing** any **cybersecurity training** or **awareness programs** to their employees in 2024.



A word from our experts

With AI-driven threats on the rise, addressing cybersecurity is no longer a choice – it is a business imperative. Companies that invest in preparation now will be the ones standing tomorrow.

Partner Andreas Schütz, LL.M., CEE Head of IT

Management liability for cybersecurity is real. With tightening regulations, leaders must ensure security is not just an IT concern, but a business-wide priority.

Partner Philipp Zumbo, CEE Head of Dispute resolution

TaylorWessing

Let’s secure your business future

We offer customized workshops and guidance to:

PROTECT - Risk assessment, compliance, and internal documentation

MANAGE - Step-by-step action plans to mitigate the immediate impact of incidents

RECOVER - Post-incident reviews and resilience building

Contact us today to explore our tailored solutions or schedule your cybersecurity workshop.

Andreas Schütz, LL.M.
Partner, IT / Data protection
Vienna
+43 1 716 55
a.schuetz@taylorwessing.com

Philipp Zumbo
Partner, Dispute resolution
Vienna
+43 1 716 55
p.zumbo@taylorwessing.com

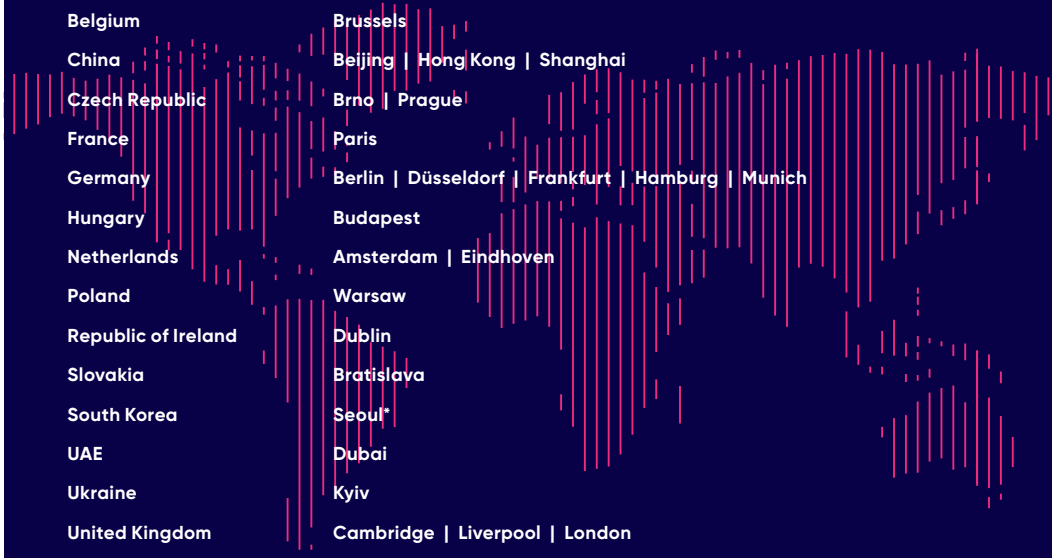
Ivo Deskovic
Partner, Dispute resolution
Vienna
+43 1 716 55
i.deskovic@taylorwessing.com

Erik Steiner
Counsel, IT
Vienna
+43 1 716 55
e.steiner@taylorwessing.com

Christopher Bakier
Senior Assoicate, IT
Vienna
+43 1 716 55
c.bakier@taylorwessing.com

TaylorWessing

1200+ lawyers
300+ partners
28 offices
17 jurisdictions



Austria	Vienna
Belgium	Brussels
China	Beijing | Hong Kong | Shanghai
Czech Republic	Brno | Prague
France	Paris
Germany	Berlin | Düsseldorf | Frankfurt | Hamburg | Munich
Hungary	Budapest
Netherlands	Amsterdam | Eindhoven
Poland	Warsaw
Republic of Ireland	Dublin
Slovakia	Bratislava
South Korea	Seoul*
UAE	Dubai
Ukraine	Kyiv
United Kingdom	Cambridge | Liverpool | London
USA	New York | Silicon Valley

* In association with DR & AJU LLC

taylorwessing.com

TaylorWessing