Directors' Liability for Cyber Incidents in Aviation: Closer than you think

Airlines are among the most digitally dependent businesses in the world. From flight planning and maintenance systems to crew management and passenger data: virtually all core processes are ICT-driven. That makes the sector an attractive target for cyberattacks. Less well known is that a cyber incident may have not only operational or financial consequences, but also result in personal liability for directors.

Airlines fall directly within the scope of the NIS2 Directive, in which the European Union explicitly designates civil aviation as an essential sector. This classification means that airlines are required to organise cybersecurity robustly all the way up to board level. As a result, directors' personal liability is no longer a theoretical issue, but a concrete risk lurking behind every cyberattack.

In this article we explain why directors in the aviation sector are increasingly exposed to personal liability, which obligations apply to them under the latest legislation, and which measures are sensible to reduce that risk.

Legislation: responsibility all the way into the boardroom

An example of this legislation is the aforementioned Network and Information Security Directive (NIS2): cybersecurity rules for entities in critical sectors. NIS2 contains cybersecurity requirements for organisations in critical sectors, including aviation. Although these rules are formally addressed to the organisation, the legislator is explicitly focusing on the role of the board.

While it is well known that a company may be liable for damage, it is less well known that directors may also be held personally liable if they can be seriously blamed. In practice, that standard is therefore increasingly shaped by compliance with laws and regulations, including NIS2.

Under this Directive, airlines must be able to demonstrate that their directors have sufficient understanding of digital risks. This is not about technical details, but about insight into threats, supply-chain vulnerabilities, and dependencies of critical systems. The board must approve cybersecurity policy, monitor implementation, and periodically evaluate it. An annual update from the CISO is therefore no longer sufficient.

Training mandatory for directors and management

The European line is clear: digital resilience must be anchored in the boardroom. That is why NIS2 requires directors to follow training in this field. Not on a voluntary basis, but demonstrably—for example through certificates. For airlines, this means that directors must understand which cyber threats are relevant, how risk analyses are performed, and how the organisation must steer on digital continuity. That obligation also rests on managers who are responsible for steering, policy, and risk management within airlines.

Anyone who thinks this obligation can be "outsourced" with a single click to the IT supplier is mistaken. The legislator explicitly states that outsourcing does not mean the board no longer bears responsibility. Ultimately, it remains the board's task to verify that the policy works, that measures are complied with, and that incidents are reported in a timely manner.

Airlines will also be subject to proactive supervision by the regulator. There is no transitional period. This means that entities to which the law applies must be compliant at the moment it enters into force. If they are not, the regulator may impose sanctions not only on the organisation itself, but also on directors.

Examples of obligations include:

- The board must have sufficient knowledge and skills to identify and manage ICT risks;
- The board must regularly follow training on ICT risk management;
- The board must approve the information security policy;
- The board must oversee implementation of the information security policy.

Approving policy and overseeing implementation

The board must map the risks the organisation faces in the field of cyber threats, establish control measures, and ensure that these measures are actually implemented within the organisation. This is not a one-off exercise for the board. Resilience against cyber threats must be a recurring agenda item for the board and should be embedded in a plan–do–act–check cycle.

Heightened duty of care

These and other obligations mean that, in practice, directors face a heightened duty of care to manage ICT risks. The absence of appropriate management and control systems, or (structurally) failing to meet training obligations, can result in serious blame and therefore directors' liability. A prudent director therefore ensures that he complies with training obligations, that a sound ICT policy has been implemented, and that his directors' and officers' liability insurance is in order.

American-style situations?

The damage from a cyber incident in aviation can be enormous: flights are cancelled, systems must be restored, passengers and partners submit claims, and reputational damage may occur. Regulators may also impose substantial fines if security obligations are not complied with. In certain cases, administrative fines may even be imposed directly on directors.

In the United States we already see numerous lawsuits against directors following cyberattacks. Although the context differs, it shows that holding directors personally accountable is no longer an exception. In the Netherlands too, partly due to the possibility of collective damages claims, this is a realistic scenario.

Examples include proceedings following liability claims against the directors of, for instance, Target, Home Depot, Wendy's and Yahoo. In the case of Home Depot this resulted in a settlement to avoid a judgment. Part of the settlement was that Home Depot would still take measures to improve cybersecurity.

It seems only a matter of time before directors in the Netherlands are also held directly liable in connection with cyber incidents. In that context it should not go unmentioned that since the entry into force of the WAMCA in 2020, it has been possible in the Netherlands to claim collective damages. This has led in recent years to various mass claims, for example for violations of the GDPR, whether or not connected to data breaches. It is expected that in the near future mass claims will follow against organisations whose digital resilience was not in order, and that directors will be involved in those proceedings.

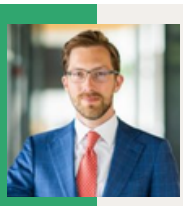
Conclusion

The pressure on directors in aviation is increasing. New EU legislation introduces obligations that affect not only the organisation, but also the individuals at the helm. Directors cannot hide behind suppliers or internal departments: they must themselves map ICT risks, approve policy, oversee implementation, make appropriate contractual arrangements, and follow mandatory training. Under NIS2, that training obligation applies to the members of the "management body" (the board, executive management, and (parts of) senior management).

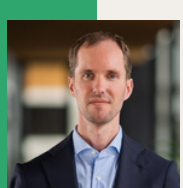
Only in this way can it be prevented that a cyber incident affects not only the airline, but also the director personally.

> Would you like to know where your organisation stands or do you need support with preparations for the Cybersecurity Act, then we will be happy to help.
>
> We also provide the legally required training for directors and management. In cooperation with Bureau Veritas Cybersecurity, we have delivered boardroom trainings for almost 100 organisations. The directors and supervisory board members who attended our training rated it on average 8.8.
>
> As a Preferred Supplier of BARIN, we are pleased to support airlines with optimal preparation for the Cybersecurity Act. Please feel free to contact us.

For more more information please contact



Menno de Wijs
| Attorney at law
IT, Privacy & Cybersecurity
m.dewijs@declercq.com
+316 41 19 48 80



Jeroen van Helden
| Attorney at law
IT, Privacy & Cybersecurity
j.vanhelden@declercq.com
+316 28 53 60 54