Cybersecurity

From senior leadership to our central team to the wider community across our businesses – we are deeply committed to ensuring strong cybersecurity.

Leading from the top

The board sets our groupwide cybersecurity policy. It has four key parts: good governance, good protection, good detection, and good response. This forms the backbone of our robust approach. We cascade the policy through the segments to the businesses, giving the businesses ultimate responsibility for making sure they implement strong cybersecurity in line with their own operations and challenges. For example, we expect each business to have the right level of incident management and crisis management to ensure a good response to any security incidents.

Central expertise

Our central cybersecurity team provides expert help and support to the segments and businesses. As part of our internal audit and risk function, the team's approach is to help the development of a competent, agile community of cyber and risk professionals. To this end, the team has three guiding principles:

1. **Cyber is an enabler, not a blocker**
2. **Help manage risk, not spread fear, uncertainty and doubt (FUD)**
3. **Every employee is a cyber warrior**

The team undertakes about 70 advisory and assurance projects a year to help ensure cybersecurity is implemented well around the world by the different businesses, in line with our groupwide policy.

Major focus areas include business resilience, the security of the platforms at the heart of the businesses and, in turn, the security embedded in the software development life cycle.

Regular reporting

The team reports to the risk and audit committees four times a year. On two occasions, it presents an extended report on how well the businesses are doing against the policy – where they are now, where they were six months ago and where they are expected to be in six months' time.

The reports for the risk committee give a comprehensive overview, including the key risks, the biggest challenges and any major incidents. Formal audit reports are provided for the audit committee. This regular reporting enables senior leadership and key governance committees to stay in touch and on top of cybersecurity.

In addition, every three months the team leader meets with the head of internal audit and the group CFO to discuss the most important cybersecurity issues and where to focus in the months ahead.

Focused help and support

The team's audit work ranges from regular informal discussions with security leaders across the group through to formal audits of businesses as and when required.

As part of its advisory brief, the team coordinates a high level of active testing, including hiring teams of ethical hackers as well as using the responsible disclosure platform to stress test defences.

The aim is to keep testing and strengthening the security and resilience of the individual businesses and group as a whole.

The team provides a range of other advisory help and support, from assessing the cybersecurity risks and strengths of a business as part of a mergers and acquisition (M&A) project through to specific issues around a particular platform upgrade or change. The emphasis is not just on providing security advice around the technology but also in terms of helping the businesses meet their challenges, make the most of their opportunities and achieve their ambitions. The ultimate aim is to help our businesses grow and succeed in a safe and secure way.

Building a strong cyber-community

We also cultivate a strong cyber-community across the group. By connecting everyone they can quickly and easily exchange updates and know-how. It's also a great way to build a shared sense of belonging to something bigger and playing an important part in the success of the group as a whole.

Every six weeks the security leads from the different businesses get together on a call hosted by the central team lead. It is a great way for everyone to discuss hot topics and share updates on key events and risks.

This coming September the first of an annual series of cyber-retreats is planned where the security leads can align on strategy and focus on the year ahead.

For the wider cyber-community across the group, an online workspace has proven to be a very popular and effective way for all the security professionals to stay in touch, discuss the latest security trends and risks, and also come together to coordinate responses to incidents.

Cultivating our cybersecurity culture

In November 2019 we held our first Cyber Forward Conference, in Amsterdam. Building on the success of this two-day event, the plan for 2020 is to hold three Cyber Labs, in Latin America, Europe and India. This will enable us to take the event around the world and introduce more experimentation and interactions around building the security and resilience of the businesses.

Looking ahead

As the group grows, we will continue to ensure that cybersecurity remains a key focus across all our businesses. We are looking to broaden and deepen our culture of cybersecurity and also to extend our capabilities. On this front, we will be exploring the creation of cyber-internships, working with a local university in the Netherlands to develop a joint six-month master's programme. It is one of the ways we are investing in the next wave of cybersecurity talent to ensure we keep growing and succeeding safely and securely.

Bringing everyone together

"We travel a lot and we see all the security people from around the group. Our job is to cross-pollinate knowledge and bring best practices to the businesses. No matter how much we share, we cannot share too much."

Trajce Dimkov
Group cyber coach

Our services at a glance

Risk-driven process reviews
- IT risk assessment
- Business resilience assessment
- SDLC assessment
- Application security assessment
- IT general controls assessment

Data-driven deep dives
- Cloud X-ray
- Data X-ray
- Process X-ray

Security testing
- Ethical hack
- Cloud ethical hack
- APT simulation

Resilience exercises
- Crisis simulation
- War gaming

Managed services
- Security posture evaluation
- Crowd-sourced vulnerability programmes