Vodafone Group Plc

Cyber Security Factsheet 2025

everyone.connected

Introduction

At Vodafone, our purpose is to connect everyone. Our connectivity is critical national infrastructure and is relied upon by millions of customers around the world. We prioritise cyber and information security across everything we do.

Cyber attacks are part of all our lives today and will be in the future. All organisations, governments and people will be subject to cyber attacks and some will be successful. The telecommunications industry is faced with a unique set of risks as we provide connectivity services and handle communication data. Our operating model and strategy are designed to manage the challenging threat landscape. We implement controls that are designed to prevent, detect, respond and recover from attacks. By taking this approach we aim to minimise impact to customers and the services we provide.

This factsheet outlines our approach to managing cyber risk at Vodafone, as well as how we protect our customers from cyber threats. Our cyber security strategy is aligned to the Company strategy and focused on the actions we need to take to protect our customers and society now and in the future.

Our cyber security strategy will continue to evolve based on changing threats, technology developments, our strategic and business priorities, and regulation. We will provide a full update on our strategy in our next cyber security factsheet.

View more online

Click to watch our Chair talk about the importance of cyber security during his Board site visit:

investors.vodafone.com/videos

Click to watch our Group Chief Executive talk about the importance of cyber security:

investors.vodafone.com/videos

Highlights

Our vision
a secure and resilient connected future for everyone

Cyber simulations
for our business leadership to be better prepared for cyber events

Over 900
in-house international team of experts

ISO 27001 certified
across our global technology function and 9 local markets

Global scale
through consistent control baseline, global telemetry and deep expertise

Independent testing
of our mobile networks every year

Collaboration
with industry, government, and standards-setting bodies

Security operations
manage billions of events globally to detect threats

Contribution to UN Sustainable Development Goals ('SDGs')

8 DECENT WORK AND ECONOMIC GROWTH

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

Contents

References

We have cross-referenced relevant material and included the navigation icons.

➔ Read more in the report

+ Click to see related content online

▷ Click to watch related content

Strategy

Our cyber security strategy

Our vision is a secure connected future for our customers and society. We are motivated by a clear purpose to inspire customer trust and loyalty by providing sustained cyber security, ultimately contributing to a secure society and an inclusive future for all.

Our cyber security strategy and operating model support our vision and goals and form part of our wider Company strategy.

Our strategy is based on core principles including:

- Act as an enabler for the business;
- Be proactive and threat-led, supported by data-driven decisions, automation, and digitisation;
- Build and assure security in all products and services; and
- Simplify architecture through partnership with key suppliers.

In the past year we have been redeveloping the strategy based on changes in the internal and external environment. This takes account of future threats and changes in technology so it remains fit for purpose over the next five years and beyond. The updated strategy consists of five main areas:

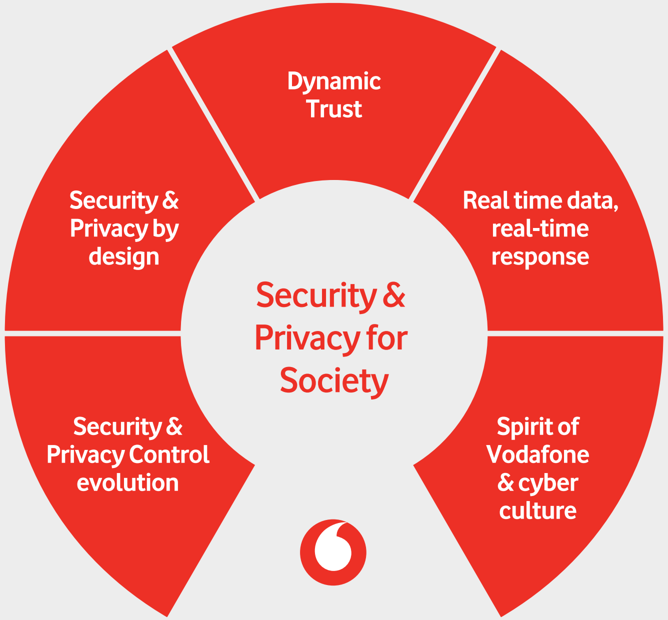
Dynamic Trust, Identity and Insider

Through robust tooling and processes, we make sure the right people can access the right information at the right time.

Proactive Health and Real-time Response

The next generation of our detection and response capability, using advanced analytics and automation to expand our capabilities.

Strategic pillars


Dynamic Trust
Real time data, real-time response
Spirit of Vodafone & cyber culture
Security & Privacy Control evolution
Security & Privacy by design
Security & Privacy for Society

Cyber Health and Adaptive Risk Method ('CHARM')

We provide a continuous view of our security risk which adapts to change and is quantified to make better risk decisions.

Securing Networks, Products & Services

New technologies are harnessed securely and products and solutions are designed with security in mind. We enable secure connectivity through an end-to-end operating model for telecoms security.

Supplier and Society Ecosystem

We embed and drive good security practice across our suppliers. We partner and collaborate widely to achieve good security outcomes for our customers and society.

Each year we define and communicate priorities for a three-year period, so all areas of the business are clear on the investment priorities for security. We track progress against these priorities throughout the year.

Year ahead

We have started work on five transformations aligned with the updated strategy. These include:

- Design and development of a new security operations platform;
- Further strengthening multi-factor authentication;
- Enhancing end-to-end security of our telecommunications networks;
- Transforming how we manage the security of our third parties; and
- Implementation of CHARM.

Alongside these priorities, we continue to focus on security control improvement, efficiency and automation.

▷ Click to listen to our experts summarise our approach to cyber security: **investors.vodafone.com/videos**

Strategy continued

New technologies and industry collaboration

We adopt new technologies to better serve our customers and gain operational efficiency. For every technology programme we follow our Secure by Design process, evaluating suppliers' hardware and software, modelling threats and understanding the risks before designing, implementing and testing the necessary security controls and procedures.

Mobile networks

Every new mobile network generation has brought increased performance and capability, along with new opportunities in security. As we deploy 5G core networks alongside our 5G radio networks, often described as 5G Standalone, we have updated our security standards to implement the latest 5G features in our core networks. We also test security in our radio networks using independent third-party testing companies.

Open RAN is a new way of building and managing radio access network ('RAN') components within telecommunication infrastructure. Instead of purchasing all the components from one supplier, we use hardware and software components from multiple vendors and integrate these via open interfaces. Over time, this will create a more competitive landscape for telecommunications equipment. We continue to collaborate with other players in the Open RAN ecosystem to improve security. This includes adding requirements to the Open RAN specification, publishing internal security standards, and benchmarking vendors against these. The first Open RAN sites are now live in the UK and Romania.

Quantum computing

We are preparing for a time when quantum computers able to break certain cryptography are available at scale. Through our joint research with IBM, we have developed a risk-based approach to mitigate the risks of existing cryptography. We are identifying where we are using cryptography that is potentially vulnerable to attack from quantum computers, defining supplier requirements and developing the ability to update our cryptography when new threats emerge. We have set up a long-term Quantum Safe programme, and plan to pilot migration activities in the next year in collaboration with IBM and telecom vendors. Vodafone co-chairs the telecommunications industry-wide task force on this issue.

Artificial intelligence ('AI')

We take the responsible use of AI seriously and seek to balance the opportunities and security risks associated with AI. Security teams from across the business are collaborating under the governance of a global responsible AI committee which agrees policy, mitigates threats, identifies and selects use cases for implementation.

To deliver secure and responsible AI, we integrate secure AI lifecycle practice, requirements and tools into strategic AI platforms and internally developed AI applications. To reduce the risks of misuse, we limit access to public AI applications. We have developed an awareness programme and updated our policies to make it clear to our employees what data must not be shared with public AI applications.

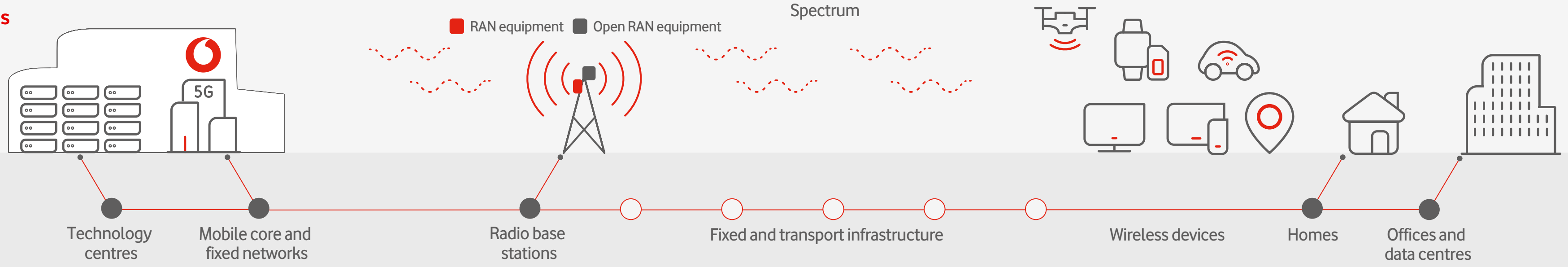
We have defined requirements for internal AI application development including risk assessment, designing for transparency, lack of bias and providing the right degree of human oversight of results. If the AI model could have a high impact on people, we require a human to have input on the final decision.

We are also experimenting with AI to augment our cyber security processes. The first application is a chatbot which can answer employee questions on cyber policies and standards. We are also engaged in cross-industry forums that collaborate on telecommunication-specific AI use cases, including threat detection, investigation and response.

Industry collaboration

We actively engage with stakeholders across industry, including regulators, standard-setting bodies and governments. Collaboration is vital to respond to threats, protect our organisation and workforce, and build safe online and digital spaces for customers and society. We use our expertise and experience to engage with a wide range of organisations to help improve the understanding of cyber security thinking and practice, and contribute to public policy, technical standards, information sharing, risk assessment, and governance. For example, we have engaged in cross-industry collaboration through the European Round Table, where we chair the CISO committee. We have an appointed member on the National Cyber Advisory Board in the UK. We also collaborate with other telecommunication companies, and actively engage in security standards working groups such as ENISA 5G Cyber Security Certification, O-RAN Alliance WG11 and GSMA Fraud and Security Group. We have a research programme working on security topics with the German Federal Ministry of Education & Research, for example on securing future generations of mobile technology.

Our Networks



Risk management

Identification of vulnerabilities and risks

Cyber attacks are part of the technology landscape today and will be in the future. All organisations, governments and people are subject to cyber attacks and some will be successful. The telecommunications industry is faced with a unique set of risks as we provide connectivity services and handle private communication data.

A successful cyber attack could cause serious harm to ourselves or our customers, including unavailability of services or a data breach leading to disclosure or misuse of customer personal data. The consequences could include, but are not limited to, exposure to contractual liability, litigation, regulatory action, or damage to the company's reputation and brand and loss of market share. In the worst case, the cyber security incident could cause material financial impact to us.

There is increasing regulatory focus on cyber security and requirements for telecommunications providers to improve their cyber security practices. We are subject to GDPR and equivalent legislation in many countries in which we operate. In addition, there are local and regional laws and regulations which impact cyber security, for example the Telecommunications Security Act in the UK and Network & Information Security 2 ('NIS2') and the Digital Operational Resilience Act ('DORA') in the EU. A cyber incident may lead to regulatory fines and other enforcement activities if deemed to be due to inadequate security. Measures to meet these laws and regulations will also result in increased compliance costs. We dedicate significant resources to reducing cyber security risks, however due to the nature of the threats, we cannot provide absolute security and some cyber security incidents will occur.

Risk and threat management are fundamental to maintaining the security of our services across every aspect of our business. We separate cyber security risk into three main areas of risk:

- **External:** A wide variety of attackers, including criminals and state-backed groups, target our networks, systems and people using a range of techniques. They seek to gain unauthorised access to steal or manipulate data or disrupt our services. Geopolitical factors also increase the threat of an external attack;
- **Insider:** Our employees may accidentally leak information or maliciously misuse their privileges to steal confidential data or to cause disruption; and
- **Supply chain:** We only have indirect control over the cyber security of third-party service providers, limiting our ability to defend against cyber threats to these third parties. Such attacks, if successful, could cause services to be unavailable or enable a data breach to occur.

To help us identify and manage emerging and evolving risks, we constantly evaluate and challenge our business strategy, new technologies, government policies and regulation, and cyber threats.

We conduct regular reviews of the most significant security risks affecting our business and develop strategies and policies to detect, prevent and respond to them. Our cyber security strategy focuses on minimising the risk of cyber incidents that affect our networks and services. When incidents do occur, we identify the root causes and use them to improve our controls and procedures.

Cyber security risk is aligned with Vodafone's enterprise risk framework. The most important risks to the company are referred to as Principal risks, of which Cyber risk is one. The risk owner produces a formal Line of Sight document that describes the risk, the risk tolerance, current position against tolerance, controls and actions to move to tolerance if required. Second and third line assurance information is also included in the document.

Risk management continued

Risk and control approach

The global Cyber and Information Security policy applies to all Vodafone-controlled entities with over 50% ownership. Each security domain has a supporting policy document with detailed control objectives. The policies are underpinned by security standards which provide relevant technical specifications.

Security controls define the measures to mitigate risk and meet our policies. These controls are designed to prevent, detect, respond to or recover from threats. Most risks and threats are prevented from occurring and we expect most will be detected before they cause harm and need a response.

Adaptive risk and control methodology (‘CHARM’)

We have launched a new global methodology for cyber security risk management which we call the Cyber Health and Adaptive Risk Method or CHARM. The goals of this approach include:

- Cyber Health – a continuous view of security based on automated key risk indicators;
- Adaptive – responds to changing threats, technology evolution and regulation;
- Risk method – quantified risk to provide better decision-making and prioritisation.

This new approach has a greater focus on risk and threats but retains the structured control framework and common targets of the former Cyber Security Baseline. Initially we are using the same control set as before under the new methodology.

To adapt to the changing threat landscape, we have defined threat and risk scenarios. The threats and associated attack techniques are mapped to the controls that most significantly reduce risk, allowing gaps to be highlighted.

We have set targets for key controls to be effective, meaning they are well-implemented and cover the relevant systems. Cyber security controls need to be continuously evolved and enhanced to mitigate risks and threats. Each year we set new annual targets, progress against the targets is monitored and reported quarterly to the senior leadership in each market and globally.

We update our priorities with changes, including any necessary new controls. The control framework will continue to evolve based on changing threats, technology developments, our strategic and business priorities, and regulation.

We have begun to automate the capture and reporting of key risk indicator data from source systems. This will reduce manual effort, be more accurate and provide stronger assurance of effectiveness. We plan to automate all relevant controls over the next two to three years.

To better quantify residual risk, we have created a risk quantification model based on threats, control effectiveness and incident data. During the current year we will start to use the outputs to help us make risk decisions.

In addition to this top-down process of risk identification and mitigation, we identify individual cyber risks at the product or system level, for example through our Secure by Design process, operational activities, scanning and monitoring, or through an incident. Risks are evaluated on a common impact and likelihood scale, mitigating actions are agreed and captured in a risk register. Any high risks identified through these processes require senior management oversight and agreement of mitigating actions.

Assurance

A dedicated assurance team reviews and validates the effectiveness of our cyber security controls, and our control environment is subject to regular internal audit. We test the security of our mobile networks every year using a specialist testing company, and they also benchmark our security against other telecommunications operators. The aim of this is to provide assurance that telecommunications controls are operating effectively. We have also appointed external specialists to perform testing on our security controls (‘red teaming’) to uncover any areas for improvement. We maintain externally audited information security certifications, including ISO 27001, which cover our global technology function and 9 local markets. In addition, our markets comply with national information security requirements where applicable. Systems going live and those undergoing change are independently penetration tested. An internal team performs some testing, and we engage third party testers where appropriate. Across Vodafone, we complete over 1,000 penetration tests every year. We also perform adversary testing exercises.

Supply chain

As well as monitoring control effectiveness within Vodafone, we oversee the cyber security of our suppliers and third parties. Controls and procedures are embedded in the supplier lifecycle to set requirements, assess risk and monitor each supplier’s security performance. At supplier onboarding, minimum security requirements are written into contracts, and we determine the inherent risk of the supplier based on the service they are providing. We then assess their controls using a questionnaire to understand the residual risk, which informs the frequency of review from annual to every three years. We follow up on open actions and ensure any security incidents are tracked and managed.

Regulatory landscape

We are seeing an increase in new security regulation as governments respond to the heightened cyber threat landscape, recognising that telecommunications operators provide critical national infrastructure. We engage directly with governments and industry partners to promote proportionate, risk-based and cost-effective solutions to security threats. We look to establish shared approaches to reinforce standardisation and regulatory frameworks that apply equally to all market participants.

In the UK, we are implementing the provisions of the Telecommunications Security Act which sets enhanced security requirements for UK network operators and their suppliers. In Europe, we are planning implementation of the NIS2 and DORA requirements. We continue to monitor the forthcoming EU Cyber Resilience Act which aims to ensure that all digital products and services fulfil basic security requirements.

The US Securities and Exchange Commission (‘SEC’) introduced cyber security incident disclosure and reporting requirements in December 2023. We updated our incident management process to include the relevant disclosure steps should a material incident occur; this is described in the Cyber Operations and Incidents section. Where applicable we have expanded these cyber security disclosures in response to the new reporting requirements.

Operating model

Our approach to cyber security

We have implemented a globally consistent cyber security operating model that is based on the leading industry security standards published by the US National Institute of Standards and Technology ('NIST'). The model is designed to reduce risk by constantly identifying threats, protecting, defending, and continuously improving our security. We operate cyber capabilities with an in-house international team of over 900 employees.

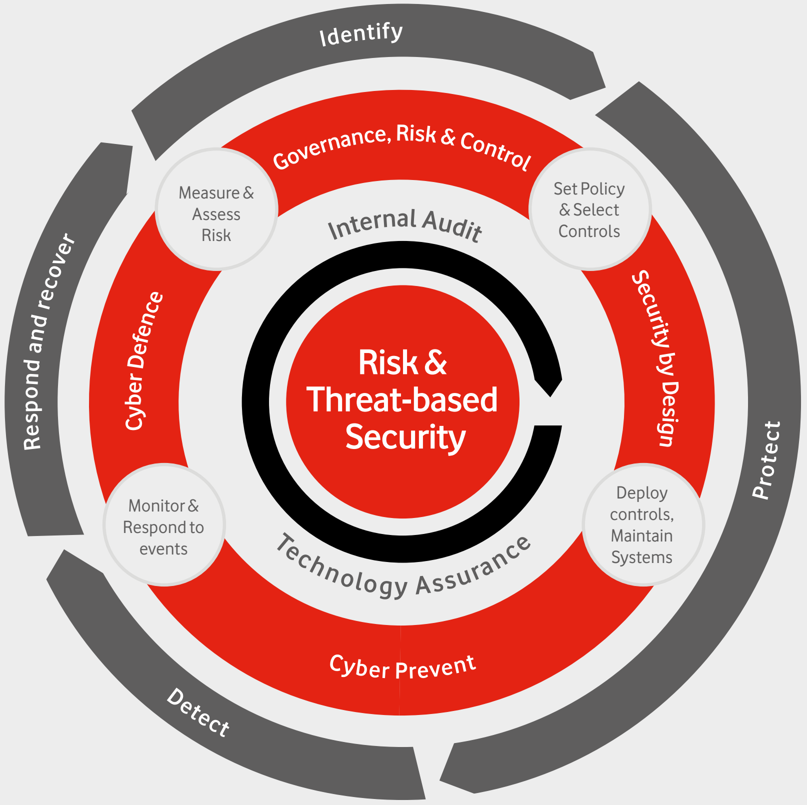
We augment our internal capabilities where necessary with third-party specialist technical expertise, such as digital forensics, red teaming and penetration testing. We use specialist resources to perform testing of our telecommunications networks. We also use qualified external resources to help during the implementation of change and improvement projects. Our scale means we benefit from global collaboration, technology sharing and deep expertise, and ultimately have greater visibility of emerging threats. An example would be our global security operations and defence capabilities which take inputs and telemetry from all the markets where we operate.

Cyber security function

Team	Responsibilities
Governance, Risk and Control	– Cyber risk framework and management across the Group. – Define and track adoption of controls and procedures, and measure effectiveness.
Strategy and Secure by Design	– Define cyber strategy aligned to technology and Company strategies. – Products, services and internal systems are secure by design.
Cyber Prevent	– Engineer, deliver and operate global security platforms, driving continuous improvement.
Cyber Defence	– Perform threat intelligence & security testing. Detect events and attacks through 24/7 monitoring. – Respond to events and incidents to minimise the impact to business and customers.
Investments & Supplier	– Manage cyber risk in Vodafone investments portfolio, partner markets, acquisitions and divestments. – Identify and reduce supplier risk.
Local Market Teams	– Responsible for managing and embedding cyber security in our local markets, including meeting local cyber regulatory and compliance requirements.

Our cyber security approach

Our cyber security approach, explained by our experts, covers the lifecycle: identify, protect, detect, respond, recover and govern. This is summarised in the video linked below.


Identify
Protect
Detect
Respond and recover
Governance, Risk & Control
Security by Design
Cyber Prevent
Cyber Defence
Measure & Assess Risk
Set Policy & Select Controls
Deploy controls, Maintain Systems
Monitor & Respond to events
Internal Audit
Technology Assurance
Risk & Threat-based Security

▷ Click to listen to our experts summarise our approach to cyber security: **investors.vodafone.com/videos**

Operating model continued

Governance

Management

The Chief Technology Officer ('CTO') and Chief Network Officer ('CNO') are the Executive Committee members accountable for managing the risks associated with cyber threats and information security. The Cyber Security and Technology Strategy & Governance ('Cyber') Director is responsible for managing and overseeing cyber security across Vodafone and reports to the CTO.

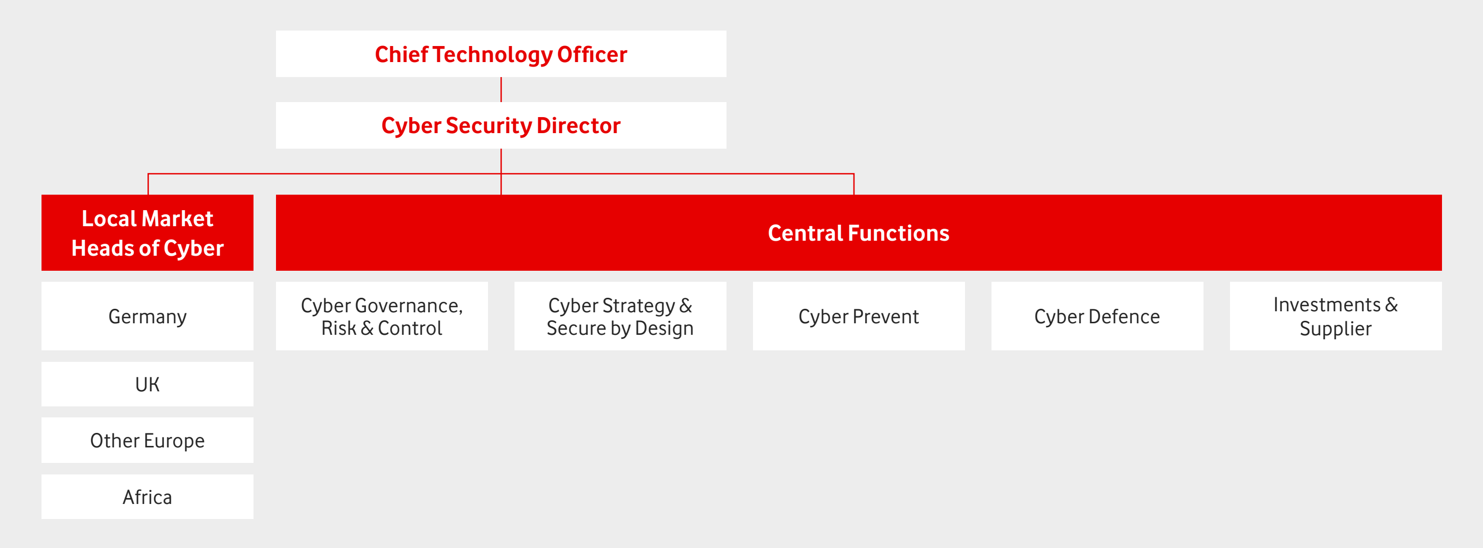
Within the cyber security organisation, led by the Cyber Director, we have heads of global cyber security functions, local markets and regional cyber security leaders. This global leadership team is responsible for directing, managing and reducing cyber risk across Vodafone. Market and regional cyber security leaders are also part of their local management teams, with a dotted matrix reporting line to local chief information officers.

The Cyber Director has led cyber security in Vodafone since 2015. Prior to joining Vodafone, the Cyber Director was chief security officer at a large UK bank, after previously holding security and technology audit leadership roles in financial services and the UK postal service. The Cyber Director is an independent advisor for a large UK retail company, a member of the UK Cabinet Office National Cyber Advisory Board and holds several other industry advisory and committee roles. Our broader cyber leadership team has significant cyber security and technology risk experience across business sectors including telecommunications, financial services and professional services.

The cyber security leadership team reviews detailed metrics monthly covering security controls status, updates about the threat landscape, and specific key risk indicators ('KRIs') for our most important controls. Examples of KRIs include results of independent network testing by third parties, vulnerability management, patching, hardening and endpoint security status, and incident metrics. Internal reporting provides a detailed view of progress and risk reduction. If markets are consistently not achieving targets, they are expected to have plans in place to recover.

Quarterly summary management reporting is provided to the technology leadership team and Executive Committee. This is supplemented by monthly control status reports which track targets and are discussed in regular meetings with local market leadership teams.

The top level Cyber and Information Security policy is approved annually by the CTO. Risk governance is provided by a quarterly Cyber Risk Council meeting, chaired by the Head of Cyber Governance Risk and Control, and attended by the Cyber Director, the Cyber leadership team and cyber security leaders from each market. The meeting reviews and approves detailed cyber policies and standards, monitors cyber risk and threat, and oversees key strategic programmes.



Chief Technology Officer

Cyber Security Director

Local Market Heads of Cyber

- Germany
- UK
- Other Europe
- Africa

Central Functions

- Cyber Governance, Risk & Control
- Cyber Strategy & Secure by Design
- Cyber Prevent
- Cyber Defence
- Investments & Supplier

Cyber security risk is also reported to and monitored by more senior committees including the Technology Audit and Risk Committee, chaired by Internal Audit, and the Vodafone Group Risk and Compliance committee, chaired by the Chief Financial Officer ('CFO'). The Cyber Director attends both of those committees to provide updates as required.

Board

The Group Audit and Risk Committee ('ARC') is the responsible committee for the oversight of risks from cyber security threats. The Committee receives updates from Internal Audit throughout the year. The ARC reviews the risk tolerance, risk position and mitigating actions for each principal risk of the company, including cyber threat.

In addition, the Committee reviews cyber risk based on papers and presentation from the CTO and Cyber Director. The report collates the data that covers all local markets' security status. The paper also typically includes threat landscape, incidents, security position, residual risk, strategy and programme progress across the Company.

The Chair of the Board's Audit and Risk Committee is the Senior Independent Director of the Board. A former CEO at a UK financial services company, he has significant experience of overseeing technology and cyber issues. Cyber security is also discussed at the Board Technology Committee which assists the Board by overseeing how technology underpins company strategy. In total, Cyber topics were covered three times at Board-level committees in FY25.

▷ Watch our Chair of the Technology Committee talk more about his role: **investors.vodafone.com/videos**

Culture, training and awareness

Training and awareness

Our cyber security awareness approach is to educate our employees to protect themselves and our customers from cyber threats. Cyber security training is mandatory as part of our Doing What's Right programme. The training module is designed by the cyber security team to inform employees of key threats and how to avoid them. The cyber leadership team are actively involved in shaping the approach and in specific employee communication. The corporate security function lead on all employee security training and they deliver the programme and materials. If the employee fails the knowledge check which is part of the training, they are required to retake the full cyber security training module. A training manual has been produced for non-employees, so they also receive the same level of awareness. Training on cyber security is also included in our induction process for new employees. We track completion rates to ensure every employee completes the mandatory training.

Cyber security training is reinforced by regular digital communications delivered via our internal social media platform, through videos and webinars. When new threats arise or become more prevalent we provide targeted advice. Examples include reminders on the use of multi-factor authentication and not to share credentials.

We perform phishing simulations across all markets and functions to raise awareness and train employees. We target at least two exercises per market or function per year. We also run multi-market simulations to allow us to compare responses consistently – these simulations cover European and African markets and Group functions. Those who click on the link in the phishing message or share their credentials receive immediate training.

We have continued to undertake incident simulations for local executive committees. In the last year we have covered seven markets including the UK, Albania, Czechia, Ireland, Romania, Portugal and Türkiye. The simulations provide CEOs and their teams a realistic and tailored experience of managing a cyber incident and exercising their responsibilities in accordance with our common approach.

Growing our skills

We enable employees in our cyber teams to maintain and grow their skills to better protect our customers. Our company learning platform hosts cyber training on technical topics, platforms and frameworks. Employees can study towards recognised information security and cyber certifications aligned to their learning plans.

Since 2020 we have organised twice yearly Cyber Connect events for our entire global cyber security team. The events include a recap of our strategy and achievements, messages from senior leadership, external industry speakers, collaborative breakout groups and technical track sessions to learn about cyber topics and best practice. We use technology to enable a hybrid experience with some attending in offices and some remote.

The Cyber Code

The Vodafone Cyber Code has been designed to simplify and explain basic security controls and procedures to all employees. The Cyber Code is embedded in our Code of Conduct and is the cornerstone of how we expect all employees to behave when it comes to best practice in cyber security. It consists of seven areas where employees must follow good security practice.

ALWAYS use multi-factor authentication for remote systems that hold sensitive information.

NEVER allow unsupported end of life systems in Vodafone infrastructure, or release unsecured products or services.

ALWAYS apply the latest security patches, close critical and high vulnerabilities and configure systems securely.

NEVER click on links or download without knowing who it is from. Report suspicious behaviour.

ALWAYS remove access when staff change roles or leave Vodafone. Secure privileged access and only use it for privileged tasks.

NEVER share or reuse your passwords. Longer is stronger.

ALWAYS classify, label and protect information you work with.

+ Click to read more about Vodafone's Cyber Code in our Code of Conduct: **vodafone.com/code-of-conduct**

Threats and incidents

Threat landscape and intelligence

An important part of our operating model is to gather intelligence and insights in order to assess threats and drive action. The cyber threat landscape continues to be volatile across all sectors, with wide-ranging threat actors ranging from individuals to nation states. Our cyber security team use industry and external analysis to help shape our controls and procedures, and drive actions. When specific vendor or new high impact vulnerabilities are reported, we drive global remediation across Vodafone.

Geopolitical instability, conflict and tensions are leading to an increase in cyber threats from state-backed and criminal threat actors. Telecommunications companies continue to be the target of state-backed actors, often to conduct government oriented or general espionage. Cross-industry and government collaboration is a key part of mitigating the evolving cyber threats.

Ransomware and data extortion attacks from criminals are common to companies of all sizes. Based on public reporting, some companies are paying ransoms, perpetuating the threat.

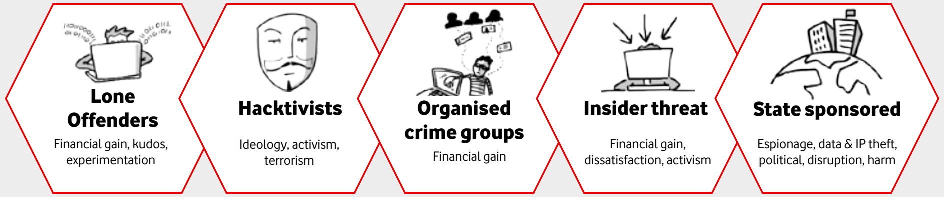
Attackers are increasingly trying to log in, rather than hack in. So-called living off the land attacks rely on the same techniques used to manage and access systems that are used widely by everyone. Detection of these attacks is more challenging. Social engineering methods are a common means for attackers to gain access. New technologies such as AI are enhancing techniques such as voice phishing and deep fakes. Harvested credentials continue to be sought and shared by threat actors. Attackers can target executives following media announcements and public reporting.

The speed of vulnerability exploitation is very fast and common. We have seen continued attacks against our suppliers, and we expect this trend will continue.

Cyber operations and incidents

As a global connectivity provider, we see a range of cyber threats. We use our layers of controls to identify and mitigate threats in order to reduce business or customer impact. Our global security operations capability handles billions of events and logs from sensors across our footprint, detecting potential threats and events. Low severity issues are dealt with quickly, for example by malware containment or isolating an individual device. More significant events are triaged to our 24/7 incident management and response team. We operate a single global team and capability.

Cyber Threat Actors



Lone Offenders
Financial gain, kudos, experimentation

Hacktivists
Ideology, activism, terrorism

Organised crime groups
Financial gain

Insider threat
Financial gain, dissatisfaction, activism

State sponsored
Espionage, data & IP theft, political, disruption, harm

Where a security incident occurs, we have a consistent incident management framework to manage our response and recovery. The focus of our incident responders is always fast risk mitigation and customer security.

In the event of a cyber breach we disclose it to the relevant authorities according to local or global regulations and laws. This may include law enforcement as well as regulators. Risk assessment of the threat actor, incident nature and potential impact to customers is important to determine the approach to disclosure. The European Union's GDPR provides a framework for notifying customers in the event there is a loss of customer data because of a data breach, and this framework is a baseline across all our markets. Our data privacy officers are a key part of the response where incidents impact personal data. We will also notify the SEC if an incident is deemed to meet their materiality threshold.

We classify security incidents on a scale according to severity, measured by potential business and customer impact. The highest severity category of event is called Severity 0 down to the lowest Severity 4. Severity 0 corresponds to a potentially significant data breach or loss of service caused by the incident. If a Severity 0 incident occurs, we notify the Executive Committee, the Board and external auditors and provide regular updates. A crisis group is formed composed of relevant senior management who oversee the response.

SEC requirements have been incorporated into our incident management process. In the event of a Severity 0 incident, the crisis group would decide whether a recommendation to the Disclosure Committee (composed of the CFO and General Counsel, among other functional leaders) is warranted. The Committee would decide if a market disclosure is necessary for materiality reasons, that would also trigger disclosure to the SEC.

Our total S1 and S2 incident volumes in FY25 were down by 29%, of which 9% is due to not reporting Spain and Italy incidents post divestment. Last year, we reported on the proportion of incidents at suppliers and third parties. In FY25, this proportion fell to 31% (FY24:55%). The main root causes of incidents were attackers exploiting weak credentials, social engineering, denial of service events and vulnerabilities being rapidly exploited.

When incidents are closed, we complete a post-incident review to learn the lessons from the incident, including the root cause and any improvements needed.

Cyber insurance is an important part of our risk management and mitigation approach. Vodafone holds cyber liability insurance alongside business interruption and professional indemnity policies.

Should a serious cyber event occur, we could recover the costs in whole or in part through these policies.

+ Click to read more about how we manage risks from technology disruptions in our SASB disclosure: **investors.vodafone.com/sasb**

Compliance with Securities and Exchange Commission cyber security disclosure requirements

The United States Securities and Exchange Commission ('SEC') introduced new cyber security reporting requirements in December 2023. We have adopted the requirements in our processes for assessing, identifying, and managing material risks from cyber security threats throughout this report. Many of the requirements were covered in our previous cyber security reporting, however this content has been moved into this report. Additionally, we have cross-referenced our disclosures to the new SEC requirements in this table.

SEC disclosure requirement	Disclosure	Page
Risk management & strategy (Form 20-F Item 16K (b))		
1. Describe the registrant's processes for assessing, identifying, and managing material risks from cyber security threats: i. Whether any such processes have been integrated into the registrant's overall risk management system or processes	Risk management > Identification of vulnerabilities and risks	Page 4
ii. Whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes, and;	Risk management > Risk and control approach > Assurance	Page 5
iii. Whether the registrant has processes to oversee and identify such risks from cyber security threats associated with its use of any third-party service provider	Risk management > Risk and control approach > Supply chain	Page 5
2. Describe whether any risks from cyber security threats, including as a result of any previous cyber security incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition	Threats and incidents > Cyber operations and incidents	Page 9
Governance (Form 20-F Item 16K(c))		
3. Describe the board's oversight of risks from cyber security threats. If applicable, identify any Board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the process by which the board or such committee is informed about the risks	Operating Model > Governance > Board	Page 7
4. Describe management's role in assessing and managing material risks from cyber security threats: i. Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant experience of such persons or members in such detail as necessary to fully describe the nature of the expertise ii. The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cyber security incidents iii. Whether such persons or committees report information about such risks to the board or a committee or subcommittee of the board	Operating model > Governance > Management	Page 7
Material cyber security incidents (Form 6-K)		
Information on material cyber security incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders	There have been no such incidents in the most recent or prior financial years.	

Vodafone Group Plc
Vodafone House
The Connection
Newbury Berkshire
RG14 2FN
England

Registered in England
No. 1833679

Telephone
+44 (0)1635 33251

vodafone.com

Contact details

Shareholder helpline
Telephone
+44 (0)371 384 2532

Investor Relations
ir@vodafone.co.uk
vodafone.com/investor

Media Relations
vodafone.com/media/contact
GroupMedia@vodafone.com

Sustainability
vodafone.com/sustainability

Online Annual Report
vodafone.com/ar2025