



INFORMATION PACK **CYBERSECURITY ENGAGEMENT**

Disclosure Examples

December 2021

ASSET MANAGEMENT

For professional investors only, not for retail investors

MINIMUM EXPECTATIONS

- Risk identification and oversight at board level
- A nominated Chief Information Security Officer (CISO) with supporting resources
- Inclusion of cyber covenants in supplier contracts and effective due diligence
- Inclusion of cyber considerations in inorganic growth strategies including in the due diligence and integration phases
- Timely disclosure of cybersecurity breaches
- Disclosures about a cyber resilient culture, to include tailored training across the workforce

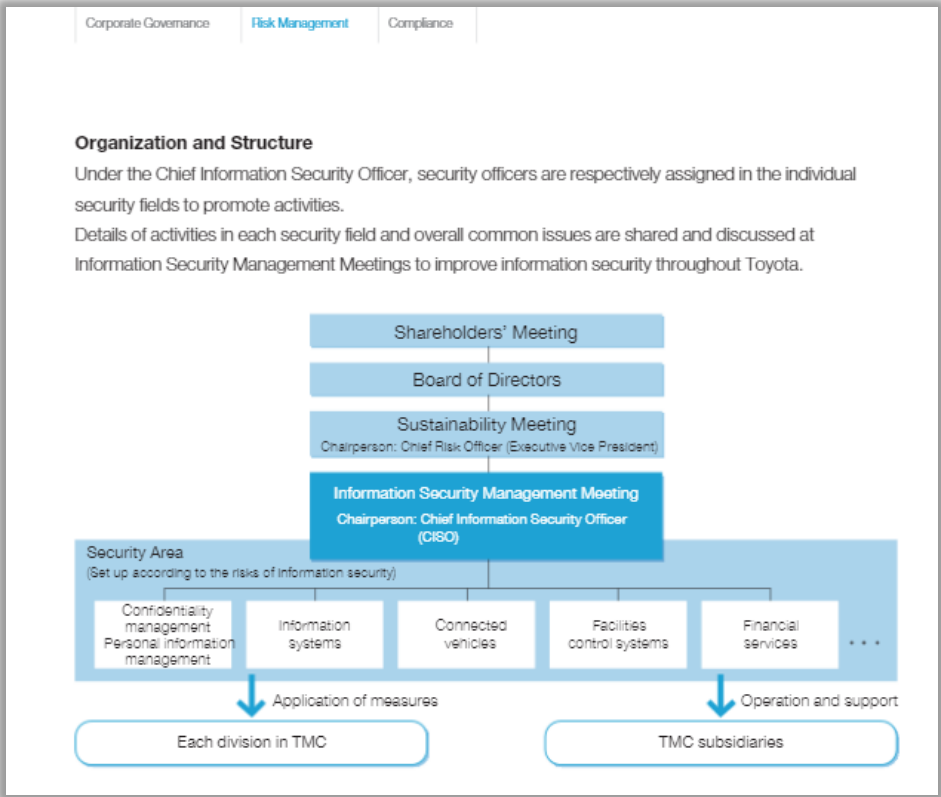
ADVANCED PRACTICES

- Inclusion of information security and cyber resilience in executive compensation KPIs
- Use of NIST Cybersecurity Framework as a reference for cybersecurity risk management
- ISO 27000 for all operations
- Evaluation of cybersecurity in board effectiveness review

CYBERSECURITY ENGAGEMENT

BOARD OVERSIGHT

ASSET MANAGEMENT



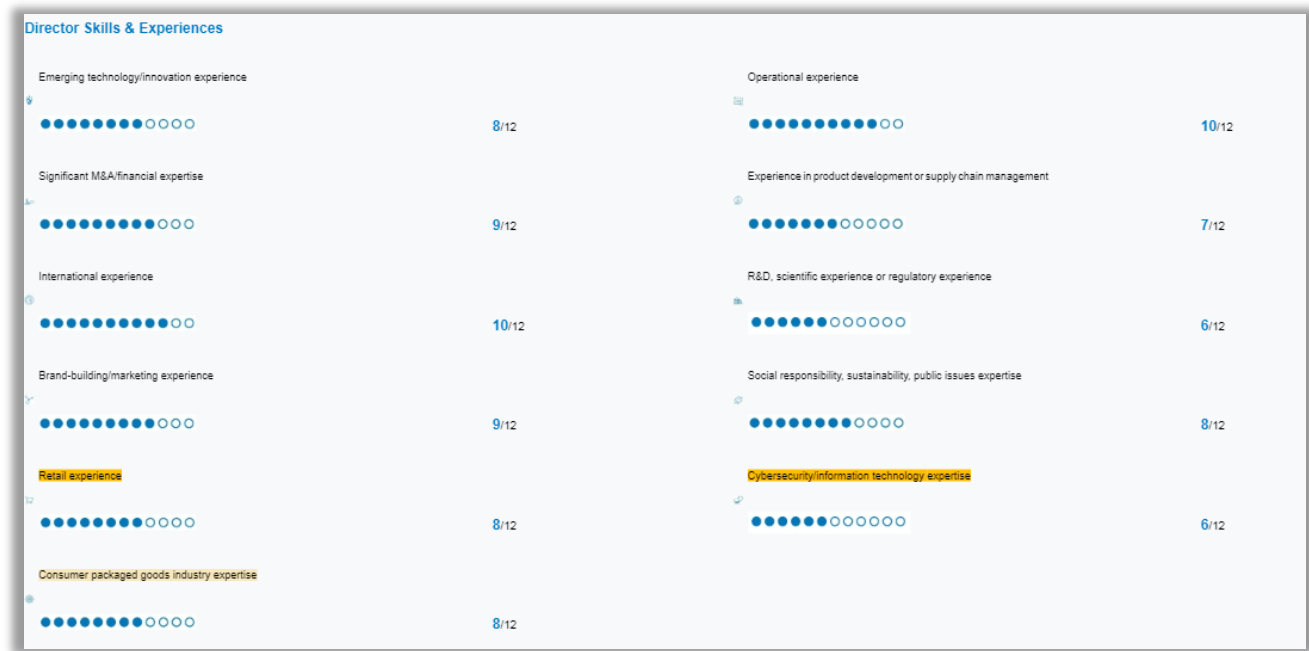
Toyota Motor's Board has a broad oversight of cybersecurity risk



Iberdrola Audit and Risk Committee have a clear mandate



CYBERSECURITY ENGAGEMENT BOARD OVERSIGHT



ASSET MANAGEMENT

Clorox Co and National Grid disclose Board skill matrix showing Board members with digital and/or cyber risk skills



2019 Effectiveness Review

The 2019 Effectiveness Review identified a number of areas on which the Board considered focus would be needed in 2020. These are summarised below, together with the resulting actions taken in 2020.

Area	Description	Summary of actions identified and taken
Board Composition	Board members to continue to consider the appropriate size of the Board and balance of skills, in particular, as a result of the Refinitiv acquisition.	As detailed in the Nomination Committee Report a number of changes were made to the composition of the Board during the year. The Report of the Nomination Committee can be found on pages: 88–90.
Stakeholder Engagement	To continue to seek improvements in stakeholder engagement.	Opportunities for in person stakeholder engagement have been more limited in 2020. See page 79 for details of in person engagement with employees and pages 68–69 for details of other stakeholder engagement.
Technology	Board to continue to find ways of improving the Board's ability to oversee and provide effective challenge on technology opportunities and threats.	The Board was provided with an increased number of updates related to technology including an update on the Group's technology strategy, cyber security and critical, strategic IT projects.
Refinitiv Integration	To continue to oversee preparations for integrating with Refinitiv.	The Board received a written and verbal update at each of its scheduled Board meeting on Integration from the COO. It also received a number of teach-ins on the Refinitiv business from the Refinitiv CEO and his leadership team.

London Stock Exchange Group plc Annual Report 31 December 2020

81

London Stock Exchange Group disclose cybersecurity as topic of focus of its Board effectiveness review

The performance measures and targets for the FY2020 Group bonus pool are set out below:

		Actual performance	Target	Performance relative to target	Maximum percentage of bonus	Actual percentage of bonus
FY2020 Group Bonus Pool	Group AOP	FY2020 AOP of £1,118m.	FY2020 AOP of £1,058m.	Above target	60%	43%
	Strategic Deliverables	<ul style="list-style-type: none"> Secured shareholder and European Commission approvals to complete the proposed Refinitiv transaction; all transaction and regulatory filings completed. Detailed planning and milestone delivery for integration is well advanced and unaffected by remote working. Agreed the €4.325bn sale of Borsa Italiana Group to Euronext N.V., securing regulatory and shareholder approvals and well-progressed separation plan to deliver the transaction in H1 2021, displaying organisational agility to execute at pace. LCH Limited recognised as a Tier 2 CCP under the EMIR 2.2 supervisory framework as part of the wider ESMA recognition of the UK framework as equivalent until at least 30 June 2022. Continued senior level advocacy with authorities in Brussels, London and Paris on equivalents and post-Brexit regulatory alignment. Further enhanced the Group's capability in operational excellence and resiliency – 2020 Cyber Security Programme, upgrade and deployment of EquityClear collateral system and execution of the Multi-Currency Clearing Platform, developed in-house, evidencing Group-wide execution capability. Cyber & Information Risk operating model across the "Three Lines of Defence" are now aligned and incorporated into the delivery roadmap for the combined company. 		Above target	40%	30%

London Stock Exchange Group includes Cybersecurity in the Remuneration Report



Embracing challenges
and changes

Admiral aims to protect its data by implementing the necessary measure to withstand a cyber-attack. In 2019 we provided all employees – including contractors – with three security training sessions. The training covered a variety of topics, which included password complexity, tailgating, risks of USB devices, data classification, suspicious emails, and phishing. In addition to this, we provided further targeted training for those identified as high-risk users.

We are also audited by external auditors on an annual basis, carry out regular security risk assessments and we operate in accordance with the NIST Cyber Security Framework.

Admiral provides training to employees and contractors and have external cyber-risk management auditors.

Quarter training released	Training provided	Coverage	Completion
Q1	Business Continuity Management	Italian Staff	98%
	Cyber Security	All Staff	99%
	EU Benchmarking Regulations	All Staff	99%
Q2	LCH Incident Management Procedure	All LCH Staff	93%
	Your Role in avoiding Tax Evasion	All Staff	
Q3	Code of Conduct	All Staff	90%
	Preventing Harassment and Discrimination	All Staff	
	Data Protection (GDPR)	All Staff	
	Privileged Access Management	IT Staff	
Q4	Conflicts of Interest	All Staff	98%
	Financial Crime & Anti-money Laundering	New Joiners	
	Preventing Bribery & Corruption	New Joiners	
	Breaking the Bias (formally known as Unconscious Bias)	All Staff	
	Gender Discrimination	Romanian Staff	

London Stock Exchange Group provides a detailed record of all quarterly training including cybersecurity



Cybersecurity risk management efforts: Metrics to monitor risk

The CERT collects more than 1 billion events from over 3,500 data sources every day, correlates them, generates about 30,000 event alerts and in the end creates about a hundred cyber incidents.

The incidents are classified according to a specific evaluation matrix (the Enel Cyber Impact Matrix), on a scale from 0 to 4, which takes their impact on company assets and the computer security tools in place into account. Most of the episodes identified do not have a significant impact on the Group's systems and are generally blocked automatically or semi-automatically, or managed by the company defenses (level 0/1).

Enel assess threats or event alerts through an impact matrix

“We operate a three-lines of defence model, aligned to the operational risk management framework, to ensure robust oversight and challenge of our cybersecurity capabilities and priorities. In the first line of defence, we have risk owners within global businesses and functions, who are accountable for identifying, owning and managing the cyber risk. They work with control owners to help ensure controls are in place to mitigate issues, prevent risk events from occurring and resolve them if they do. These controls are executed in line with policies produced by the information security risk teams, the second line of defence, which provide independent review and challenge. They are overseen by the third line of defence, which is the independent internal audit function.”

HSBC three-line of defence model

To minimize cybersecurity risks, such as tampering or unauthorized access to critical corporate data, we have implemented **security concepts**. These include access controls, security measures to protect the interfaces of our secure networks, and adequate protection of Fresenius terminals (e.g., desktops, servers, mobile devices, etc.). We also carry out regular penetration tests for applications that work with sensitive data (e.g., patient or employee data). We maintain redundant systems for all critical systems, such as communications infrastructure or clinical information systems. A central Cybersecurity Dashboard acts as a platform to analyze current and emerging threats to our critical information assets and systems. To respond more efficiently to cybersecurity incidents, we intend to roll out this dashboard further, and to introduce additional automated response mechanisms. In 2019 for instance, we implemented the automatization platform “Phantom” to automatically react to potential cyber threats.

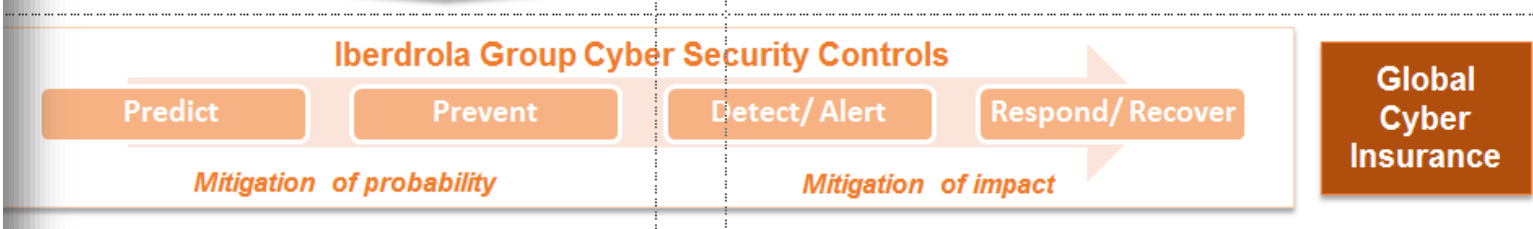
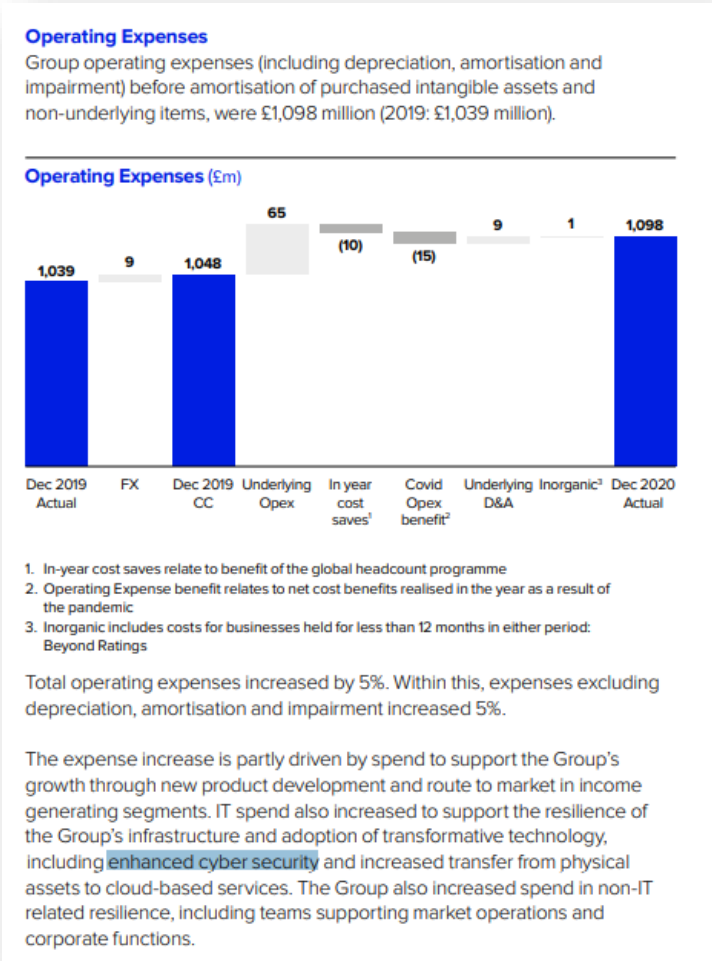
Fresenius discloses a range of management action to reduce cybersecurity risks.

CYBERSECURITY ENGAGEMENT

RISK MANAGEMENT

Cybersecurity risk management efforts

ASSET MANAGEMENT



Iberdrola includes a cyber insurance policy in its management strategy

London Stock Exchange Group includes cybersecurity costs in its OPEX analysis



Moreover, the Enel Group carries out an active vulnerability research through the execution of (hundreds of) assurance checks (Ethical Hacking, vulnerability assessments, penetration tests, etc.) with the aim to identify possible weaknesses before the possible exploitation of them by potential cyber attackers. This is done not only through automated tool but also through the deep knowledge provided by a team of selected cyber security experts.

Enel hires external cyber security experts.

Siemens Healthineers uses ISO Standards to certify its Information Security Management and uses its membership in the Charter of Trust as a source of external advice to improve supply-chain management.

<https://www.charteroftrust.com/about/>

A.6.2.2 Operational risks

Cybersecurity

We observe a global increase of cybersecurity threats and higher levels of professionalism in cybercrime, which pose a risk to the security of products, systems and networks and the confidentiality, availability and integrity of data. The increasing capabilities of state-sponsored hacking and professionalization of attacks contribute to a growing cybersecurity risk in particular to the healthcare sector, which is subject to specific privacy regulations with regard to a wide range of health information. These threats, if they materialize, could lead to major negative impacts on our business, performance and reputation. On a global level we can see rising political interest in cybersecurity, caused by increasing cyber risks in a highly complex technological environment. As a result, compliance with existing and emerging cybersecurity-specific laws and regulations on a local or regional level must be ensured. Any breach of these regulations could lead to financial and reputational damages that can be avoided only with a strong internal control system and high awareness for the relevant requirements and risks. As with other large multinational companies and our own customers, we have also been subject to targeted social engineering and sophisticated phishing attacks that we were able to identify and stop with our established technical and organizational controls. As we expand our business portfolio and leverage digital technologies including the digitalization of our supply chain, our cyber-resilience has become a key business enabler that is important to sustain. Therefore, we continue to focus on expanding, adapting and improving established security controls across the organization. Contributing measures include among others the certification in Information Security Management according to ISO Standard 27001, the implementation of new security technologies in our IT infrastructure and the continuous improvement of our provider security management. By adhering to and supporting the Charter of Trust for a secure digital world, we are on track to systematically improve the supply chain security, further adapt our security by

Each day in 2018, the CERT enabled Enel to block: > 2.3 million incoming e-mails (malicious or spam); > 300 viruses; > 740,000 outgoing risk connections; > 340 attacks on Group portals.

Enel detects over 1,000 Internet domains for the illegal use of the brand and over 100 hostile interventions each year using threat intelligence services.


In 2018, approximately 500 systematic verification activities ("Ethical Hacking") were carried out, on a protection level achieved by IT and industrial systems and applications.

Enel discloses data on its efforts to prevent cyber attacks.

CYBERSECURITY ENGAGEMENT
STATEMENTS ON CYBERSECURITY RISK

ASSET MANAGEMENT

Standalone statement/policy



Corporate Risk Policies | 1

Corporate Risk Policies

28 April 2020

Corporate Credit Risk Policy	DS	2
Corporate Market Risk Policy	DS	2
Operational Risk in Market Transactions Policy	DS	2
Insurance Policy	DS	2
Investment Policy	DS	2
Financing and Financial Risk Policy	DS	3
Treasury Share Policy	DS	3
Risk Policy for Equity Interests in Listed Companies	DS	3
Purchasing Policy	CC GD DS C	3
Information Technology Policy	DS	4
Cybersecurity Risk Policy	DS	4
Reputational Risk Framework Policy	DS	5

Cybersecurity Risk Policy

The *Cybersecurity Risk Policy* establishes a global framework for the control and management of the cybersecurity risks applicable to all the companies of the Group. In particular, it refers to the risks arising from threats and vulnerabilities affecting the Group's control, information technology and communications systems, as well as any other asset forming part of its cyber-infrastructure. It also establishes the guidelines for a common cybersecurity management model for the entire Group, coordinated by a Cybersecurity Committee and based on the development of global rules and standards to be applied within all the businesses and corporate functions, thus encouraging a strong culture of cybersecurity.

The *Cybersecurity Risk Policy* is based upon the following basic principles:

- Raising awareness among all employees, contractors and collaborators regarding cybersecurity risks and ensuring that they have the knowledge, skills, experience and technological abilities needed to support the Group's cybersecurity goals.
- Ensuring that the Group's information technology and communications systems have an appropriate level of cybersecurity and cyber-resilience and applying the most advanced standards to those that support the operation of critical cyber-infrastructure.
- Fostering the existence of appropriate cybersecurity and cyber-resilience mechanisms for the systems and operations managed by third parties that provide services to the Company.
- Strengthening capacities for prevention, detection, reaction, analysis, recovery, response, investigation and coordination against terrorist activities and criminality in cyberspace.
- Providing procedures and tools that permit rapid adaptation to changing conditions in the technological environment and to new threats.
- Collaborating with the relevant governmental bodies and agencies in order to contribute to the improvement of cybersecurity in the international sphere.
- Promoting the principles established in the *Policy*.
- Protecting the information regarding the Group's critical cyberinfrastructure and cybersecurity systems.
- Implementing cybersecurity measures based on efficiency standards.
- Acting in accordance with applicable law and the *Code of Ethics*.

The *Cybersecurity Risk Policy* sets out the Company's commitment to clearly and transparently report on its risks and incidents in the area of cybersecurity, in accordance with the provisions of law. Non-public Cybersecurity risks and incidents directly or indirectly relating to the Company or any other company of the Group and that could have an appreciable effect on the price of Company's shares or of any other security that the Compliance Unit defines as an affected security, might constitute inside information, as this term is defined in the *Internal Regulations for Conduct* in the Securities Markets, in which case the Company must report them to the market through the National Securities Market Commission upon the terms required by law.

Until said information is public, those persons who are aware of the existence of the risk or incident in question shall be deemed insiders, within the meaning of the provisions of the *Internal Regulations for Conduct in the Securities Markets*, may not engage in

Iberdrola has a separate cybersecurity risk policy amongst its corporate risk policies



CYBERSECURITY ENGAGEMENT

GENERAL “Zero Trust Architecture”

ASSET MANAGEMENT

(k) the term “Zero Trust Architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.

[Executive Order on Improving the Nation's Cybersecurity | The White House](#)