Cyber Risks Insurance

Coverage Summary

EssilorLuxottica

April 17th, 2024

Comparison Background

The following is a high-level scope of cover summary of cyber insurance.

Disclaimer

This is a high-level, non-exhaustive summary which should not be relied upon in substitution for the actual policy wording. Coverage will be provided by the insurers subject to the precise circumstances behind any insurance claim and upon observance of all policy terms and conditions.

Cyber Program Description

Named insured: EssilorLuxottica SA

“Company” insured: EssilorLuxottica SA or any subsidiary

"Subsidiary" means any entity of which the company stated as the insured in the Schedule has majority ownership on or before the inception date.

Exclusion of Grandvision: insurers will not make any payment under the Policies in respect of any claim made against, sums incurred by, or loss sustained by, Grandvision B.V.

Period of Insurance: 01 March 2024 to 01 March 2025, both Days at 00:01 local standard time at the principal address of the Insured

Limit of Liability: Various, see Limits of Liability

Territorial Limits: Worldwide

Description of Coverage:

This Cyber insurance Policy covers the losses relating to damage to, or loss of information from, IT systems and networks. It covers a direct (or first party) financial loss to you or your business arising from a cyber event. Third-party cyber liability insurance helps pay for lawsuits caused by data breaches on a client's network or systems.

Structure – Limits – Self Insured Retention

	Limit Layer	Cumulative Limit	Carrier
Self Insured Retention	€ 5M		n.a.
Primary	€ 10M x € 5M	€ 10M	MS Amlin 99,06% CFC Underwriting Ltd 0,94%
First Excess	€ 10M x € 10M	€ 20M	CFC Underwriting Ltd 100%
Second Excess	€ 35M x € 20M	€ 55M	CyXs 100% (led by Canopius)
Third Excess	€ 5M x € 55M	€ 60M	Brit Syndicate 100%

Cyber Incident Response

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Discovery of: ▪ **Unauthorised system access** ▪ **Electronic attack** ▪ **Privacy breach**	**Incident response management costs**	Costs incurred: a. to gain access to CFC 24/7 cyber incident response hotline; b. engage cyber incident management to coordinate the initial response to the event; c. to obtain initial advice and consultancy including threat intelligence in relation to the cyber event; and d. to obtain initial remote support and assistance from CFC's cyber incident manager to respond to the cyber event
	Legal and regulatory costs	Costs incurred to: a. obtain legal advice to determine the correct course of action; b. draft privacy breach notification letters, substitute notices, website notices or e-mail notification templates; c. notify any appropriate governmental, regulatory, law enforcement, professional or statutory body; d. respond to any regulatory investigation; and e. defend any regulatory action
	IT security and forensic costs	Costs incurred to: a. identify the source and scope of the cyber event; b. obtain initial advice to remediate the impact of the cyber event; c. conduct a forensic investigation of your critical systems; d. contain and remove any malware discovered on your critical systems; and e. engage with an IT security consultant to provide expert witness testimony
	Crisis communication costs	Costs incurred: a. to obtain crisis communications consultant's specific advice in direct relation to the cyber event; b. for the coordination of media relations in response to the cyber event; c. in respect of training for relevant spokespeople with respect to media communications; and d. for formulation of a crisis communications plan to reduce damage to brand and reputation
	Privacy breach management costs	Costs incurred for: a. notification of affected individuals, b. credit & identity monitoring, c. call-centre, d. translation services to manage communications with affected individuals

System Damage and Rectification Costs

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Discovery of: ▪ **Unauthorised system access** ▪ **Electronic attack** ▪ **Privacy breach** ▪ **Operator error** ▪ **Other non-physical peril**	**Sums incurred to repair and restore the data and your damaged critical systems**	Costs incurred: a. cost of employing contract staff or overtime costs for employees to rebuild your data, including data re-entry or data re-creation; b. cost of employing specialist consultants, including IT forensic consultants, to recover your data or applications; and c. cost of employing specialist consultants or overtime costs for employees working within your IT department to reconstitute your critical systems

System Business Interruption

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Interruption of insured's business operations caused by a system outage affecting the insured resulting from: ▪ Unauthorised system access ▪ Electronic attack ▪ Privacy breach ▪ Operator error ▪ Other non-physical peril	**Direct loss of profits** **Additional expenditure** (costs designed to minimise the direct loss of profits and maintain continuity of business, subject to such costs being less than the direct loss of profits saved	Direct loss of profits Additional expenditure including:: a. costs of sourcing your products or services from alternative sources in order to meet contractual obligations; b. costs of employing contract staff or overtime costs for employees; c. additional costs of employing specialist consultants, including IT forensic consultants to diagnose the source of the system outage; and d. overtime costs for employees working within your IT department to diagnose and fix the source of the system outage

Technology Supply Chain Failure

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Interruption of insured's business operations caused by a system outage affecting insured's technology supply chain partner resulting from: ▪ Unauthorised system access ▪ Electronic attack ▪ Privacy breach ▪ Operator error ▪ Other non-physical peril	**Direct loss of profits** **Additional expenditure** (costs designed to minimise the direct loss of profits and maintain continuity of business, subject to such costs being less than the direct loss of profits saved	Direct loss of profits Additional expenditure including:: a. additional costs of sourcing your products or services from alternative providers to meet contractual obligations; b. increased cost of sourcing the technology services that have been interrupted from a temporary third party provider; c. third party costs required to switch your systems to a new provider in the event that the technology supply chain partner cannot be restored within the indemnity period; and d. costs of employing contract staff or overtime costs for employees in order to continue your business operations.

Network Security and Privacy Liability

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Claim arising out of: ▪ **Unauthorised system access** ▪ **Electronic attack** ▪ **Privacy breach** that results in a breach of Network Security or Privacy (see cover details for reference)	**Damages** ➢ All sums which you become legally obliged to pay (including the establishment of any consumer redress fund and associated expenses) ➢ Costs and expenses incurred subject to cyber incident manager's prior written agreement	Breach of Network Security: a. the transmission of malware to a third party's computer system; b. your critical systems being used to carry out a denial of service attack; c. your failure to prevent unauthorized access to information stored or applications hosted on your critical systems or a technology supply chain partner's system; and d. identity theft, experienced by your employees, senior executive officers or any third party Breach of Privacy: a. a disclosure of or unauthorized access to any Personally Identifiable Information (PII), including Protected Health Information (PHI) and biometric data; b. a failure to adequately warn affected individuals of a privacy breach; c. a breach of any rights of confidentiality; d. a breach of any provisions of a non-disclosure agreement or breach of a contractual warranty relating to the confidentiality of commercial information, PII or PHI; e. a breach of any part of your privacy policy; and f. disclosure of or unauthorized access to your data or data for which you are responsible

Regulatory Fines

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Regulatory investigation arising out of: ▪ Unauthorised system access ▪ Electronic attack ▪ Privacy breach	➢ **Fines and penalties** ➢ **Costs and expenses incurred subject to cyber incident manager's prior written agreement**	**Regulatory investigation:** a formal hearing, official investigation, examination, inquiry, legal action or any other similar proceeding initiated by a governmental, regulatory, law enforcement, professional or statutory body against you

PCI Fines, Penalties and Assessments

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Payment card breach	➢ **Fines, penalties and card brand assessments** ➢ **Costs and expenses incurred subject to cyber incident manager's prior written agreement**	**Payment Card Breach:** an actual or suspected unauthorised disclosure of payment card data stored or processed by you arising out of an electronic attack, accidental disclosure or the deliberate actions of a rogue employee

Cyber Extortion

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Discovery of an extortion demand arising out of an extortion threat	➢ **Ransom Amounts**	**Extortion Threat:** A threat to: a. introduce malware, or the actual introduction of malware, including Ransomware, into your critical systems; b. prevent access to your critical systems or data or any third party systems hosting your applications or data, including technology supply chain partners; c. reveal your confidential information or confidential information entrusted to you; or d. damage your brand or reputation by posting false or misleading comments about you on social media sites

Hardware Replacement Costs

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Discovery of: ▪ **Unauthorised system access** ▪ **Electronic attack** ▪ **Privacy breach**	**Costs to replace computer hardware forming part of insured's critical systems damaged due to:** ➢ Unauthorised system access ➢ Electronic attack ➢ Privacy breach (subject to the economic test)	Costs to replace computer hardware forming part of Your critical systems where such systems have been damaged due to a cyber event (subject to the economic test). The cover does not apply to industrial machinery and operational technology

Media Liability

POLICY TRIGGERS	SCOPE OF COVER	COVER DETAILS
Infringement of intellectual property rights (not including patents) or defamation arising out of media content.	**All sums which you become legally obliged to pay (including liability for claimants' costs and expenses)**	**Covered within the captive layer** but not followed on the layers above

NOTABLE EXCLUSIONS (please refer to policy wording for a full description of what is excluded)

Cover	Limit & deductible
Associated Companies	In respect of any claim made by ▪ any company in which the (insured) company has greater than a 10% executive or financial interest, unless the claim emanates from an independent third party; ▪ any entity which has greater than a 10% executive or financial interest in the (insured) company, unless the claim emanates from an independent third party; or ▪ on behalf of the company against a third party.
Specified Entities	▪ In respect of any claim made against, sums incurred by, or loss sustained by, Grandvision B.V.
Wilful or dishonest acts of senior executive officers	▪ arising directly or indirectly out of any wilful, criminal, malicious or dishonest act, error or omission by a senior executive officer.
Power failure	▪ arising directly or indirectly from any failure in the power supply, including that caused by any surge or spike in voltage, electrical current or transferred energy.
Core internet infrastructure failure	▪ arising directly from a failure, material degradation or termination of any core element of the internet, telecommunications or GPS infrastructure that results in a regional, countrywide or global outage of the internet, including a failure of the core DNS root servers, satellite network or the IP addressing system or an individual state or non-state actor turning off all or part of the internet
Biometric Privacy Laws	▪ arising directly or indirectly out of any actual or alleged violation of any law or regulation relating to the processing of biometric information. For the avoidance of doubt, any unauthorised disclosure of biometric data is not excluded – see definition of "privacy breach" trigger.

Misleading advertising	▪ arising directly or indirectly from any actual or alleged false or misleading advertisement, promotion or product description
Patent infringement	▪ arising directly or indirectly out of the actual or alleged infringement of any patent or inducing the infringement of any patent
Theft of funds	▪ for theft of money or financial assets in any format, including but not limited to cash, bank notes, electronic currency, customer account balances, and stock or bond certificates.
War	▪ arising directly or indirectly out of: a. war, invasion, acts of foreign enemies, hostilities or warlike operations (whether war is declared or not), civil war, rebellion, insurrection, civil commotion assuming the proportions of or mounting to an uprising, military or usurped power; or b. any action taken in controlling, preventing, suppressing or in any way relating to a. above
Excluded territories (captive and first excess)	▪ In respect of: a. that portion of any financial loss sustained by; or b. any claim made, by any individual or entity located or domiciled in Ukraine, Russia or Belarus
Excluded territories (second excess and above)	▪ In respect of: a. that portion of any financial loss sustained by; or (a) **Company**;(b) **Subsidiary**;(c) **Third party**; or (d) **Employees**, which is/who are located in Russia, Belarus or Ukraine b. All financial loss where the **cyber event** first occurs on **critical systems** located in Russia, Belarus or Ukraine
Specific data breach	▪ Arising from or in any way connected to the notice of a data breach received by Essilor Luxottica on 7 November 2022

CLAIM SETTLEMENT ADJUSTMENT CLAUSE	▪ **First excess**: if CFC is required to pay any amount where our contribution exceeds EUR 2,500,000 in respect of any one of the following: a) Claim Reference: B169810663P23ABB b) Claim Reference: B169810663P23ACB c) Claim Reference: B169810663P23ADB d) Claim Reference: B169810663P23AEB e) Claim Reference: B169810663P23AFB f) Claim Reference: B169810663P23AHB g) Claim reference: B169810663P23ZZB (Block file) the Insurer shall has the right to apply an additional premium of 8% against the amount of the entire contribution to be paid, including costs and expenses, in respect of such Claims Reference. ▪ **Second excess**: If CyXs is required to pay any amount where our contribution exceeds EUR 8,750,000 in respect of any one of the following: h) Claim Reference: B169810663P23ABC i) Claim Reference: B169810663P23ACC j) Claim Reference: B169810663P23ADC k) Claim Reference: B169810663P23AEC l) Claim Reference: B169810663P23AFC m) Claim Reference: B169810663P23AHC n) Claim reference: B169810663P23ZZC (Block file) the Insurer shall has the right to apply an additional premium of 4,7% against the amount of the entire contribution to be paid, including costs and expenses, in respect of such Claims Reference.

About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organisational resilience, motivate your workforce and maximise performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.