CLAIMS

1. A system for cybersecurity risk management for at least one organisation comprising:

a vulnerability prioritisation module (3) operably configured for automatically identifying, and correlating, one or more cyber assets (1) of an information technology (IT) environment, a plurality of cybersecurity vulnerabilities (2), and threat intelligence (2a) related to the cybersecurity vulnerabilities (2), to determine at least one vulnerability risk score (4) for the organisation, and prioritising one or more cyber risks based on the vulnerability risk score (4);

a threat analysis module (11) for linking one or more attack techniques based on the priority of the one or more cyber risks determined by the vulnerability prioritisation module (3) for assessing a security level of a control technique of the organisation; and

a quantification module (12) operably for calculating cyber resiliency (5) based on the vulnerability risk score (4) of the one or more cyber risks, and quantifying the one or more cyber risks through a quantification model of the quantification module (12);

wherein

the vulnerability prioritisation module (3) identifies one or more cyber assets (1) to be assessed and prioritises cyber risks according to their vulnerability risk score (4);

the threat analysis module (11) is configured to filter the threat intelligence (2a) based on results of the vulnerability prioritisation module (3) to identify relevant threats; and

the quantification module (12) is further configured to receive data from both the vulnerability prioritisation module (3) and the threat analysis module (11) to optimise the quantification model, which comprises a Bayesian inference model that calculates a posterior distribution of cyber resiliency by at least using the vulnerability risk scores (4), and a Monte Carlo Markov Chain (MCMC) model that samples from

the posterior distribution of cyber resiliency, for quantification of the cyber risks for the organisation.

2. The system according to claim 1, further comprising a database for storing one or more cyber assets (1).

3. The system according to claim 2, wherein the vulnerability prioritisation module (3) is operably configured to communicate with the database for receiving the one or more cyber assets (1).

4. The system according to any one of the preceding claims, wherein the vulnerability prioritisation module (3) prioritises the one or more cyber risks with a higher vulnerability risk score (4).

5. The system according to any one of the preceding claims, wherein the threat analysis module (11) is configured to

receive threat intelligence data related to one or more cyber threats (9), and

analyse the threat intelligence data related to the one or more cyber threats (9), wherein the cyber threats (9) comprise real-world threats.

6. The system according to claim 5, wherein the real-world threats comprise at least one or a combination of Ransomware, Supply Chain, Insider Threat, Business email compromise (BEC), Distributed Denial-of-Service (DDoS) Attack, Misconfiguration, Phishing, Malware -Non-Ransomware, and Data Espionage.

7. A method for cybersecurity risk management for at least one organisation, wherein the method comprises the steps of:

automatically identifying, and correlating, via a vulnerability prioritisation module (3), one or more cyber assets (1) of an information technology (IT)

environment, a plurality of cybersecurity vulnerabilities (2), and threat intelligence (2a) of the cybersecurity vulnerabilities (2) to determine at least one vulnerability risk score (4) for the organisation;

prioritising, via the vulnerability prioritisation module (3), one or more cyber risks based on the vulnerability risk score (4);

linking, via a threat analysis module (11), one or more attack techniques based on the priority of the one or more cyber risks determined by the vulnerability prioritisation module (3) for assessing a security level of a predefined control technique of the organisation;

calculating, via a quantification module (12), a cyber resiliency (5) based on the vulnerability risk score (4) of the one or more cyber risks; and

quantifying the one or more cyber risks, through a quantification model of the quantification module (12)

wherein

the vulnerability prioritisation module (3) identifies one or more cyber assets (1) to be assessed and prioritises cyber risks according to their vulnerability risk score (4);

the threat analysis module (11) is configured to filter the threat intelligence based on results of the vulnerability prioritisation module (3) to identify relevant threats; and

the quantification module (12) is further configured to receive data from both the vulnerability prioritisation module (3) and the threat analysis module (11) to optimise the quantification model, which comprises a Bayesian inference model that calculates a posterior distribution of cyber resiliency by at least using the vulnerability risk scores (4), and a Monte Carlo Markov Chain (MCMC) model that samples from the posterior distribution of cyber resiliency, for quantification of the cyber risks for the organisation.

8. The method according to claim 7, further comprising the step of allowing the vulnerability prioritisation module (3) to receive one or more cyber assets (1) from a database.

9. The method according to any one of claims 7 or 8, wherein the threat analysis module (11) is configured to perform the steps of

receiving the threat intelligence data related to one or more cyber threats (9), and

analysing the threat intelligence data related to the one or more cyber threats (9),

wherein the cyber threats (9) comprise real-world threats.