

SYSTEM AND METHOD FOR CYBERSECURITY RISK MANAGEMENT

FIELD OF INVENTION

- 5 The invention relates to cybersecurity risk management. More particularly, the invention relates to a system and a method of cybersecurity risk management.

BACKGROUND OF THE INVENTION

- 10 As the internet becomes more complex and interconnected, it also becomes more vulnerable to cyberattacks. These attacks can vary from stealing data to disrupting operations, and they can have a devastating impact on businesses and organisations. Hence, in this era of digital transformation, the threat of cyberattacks is more real than ever.

15

There have been many high-profile data breaches in recent years, such as the SolarWinds breach, Microsoft's DNS vulnerability, and the VMWare ESXi vulnerability. These breaches demonstrate the importance of having an effective cybersecurity program in place.

20

Every organisation needs to share data and collaborate with different organisations at some point, for business reasons. Therefore, evaluating cyber risk becomes inevitable, considering the increase in the number of third-party attacks happening nowadays.

- 25 Cyber risk scores help assess the risk appetite of organisations based on which, informed decisions can be made. Assets with higher risk scores should be monitored closely to avoid potential threats.

One such invention disclosing a cybersecurity solution is disclosed in US patent no.

11438362. The patent '362 discloses a process involving scanning the assets, generating vulnerability scanning results, and analysing them in the context of various environmentally dependent factors.

- 5 Another such invention related to cybersecurity assessment is disclosed in US patent 10387657. The patent '657 discloses a system and method for evaluating cybersecurity risks within an organisation's technological infrastructure.

However, the systems disclosed in the patents '362 and '657 do not link tactics and
10 techniques used by attackers to hamper the security control, which could be further used for assessing the strength of the controls.

Therefore, there is a need for a system and a method which automatically identifies and gathers information about assets and combines that information about vulnerabilities
15 with data from threat intelligence sources to determine the risk level of each vulnerability.

SUMMARY OF INVENTION

- 20 The objective of the present invention is to provide a system for cybersecurity risk management which may overcome the drawbacks discussed above.

In an aspect of the present invention, a system for cybersecurity risk management is disclosed.

25

In one embodiment of the present invention, the system comprises a vulnerability prioritisation module, a threat analysis module and a quantification module.

More specifically, the vulnerability prioritisation module is operably configured for

correlating one or more cyber assets, a plurality of cybersecurity vulnerabilities, and threat intelligence related to the cybersecurity vulnerabilities, to determine a vulnerability risk score and prioritising one or more cyber risks based on the vulnerability risk score.

5

Further, the threat analysis module is configured for linking one or more attack techniques, based on the priority of the one or more cyber risks determined by the vulnerability prioritisation module. The threat analysis module is operably configured to assess a security level of a predefined control technique.

10

Moreover, the quantification module comprises a quantification model for calculating cyber resiliency based on the vulnerability risk score of the one or more cyber risks and quantifying the one or more cyber risks.

15 More specifically, the quantification module is further configured to receive data from both the vulnerability prioritisation module and the threat analysis module to optimise the quantification model, thereby enabling optimal quantification of the one or more cyber risks.

20 In the embodiment of the present invention, the system comprises a database for storing one or more cyber assets.

More specifically, the vulnerability prioritisation module is operatively configured to communicate with the database for receiving the one or more cyber assets.

25

In another embodiment of the present invention, the vulnerability prioritisation module prioritises the one or more cyber risks with a higher vulnerability risk score.

Additionally, the vulnerability prioritisation module identifies the one or more cyber

assets to be assessed.

In the embodiment of the present invention, the threat analysis module is configured to receive threat intelligence data related to one or more cyber threats. Further, the threat
5 analysis module analyses the threat intelligence data related to the one or more cyber threats. The cyber threats comprise real-world threats.

In another embodiment of the present invention, the real-world threats comprise at least one or a combination of Ransomware, Supply Chain, Insider Threat, Business email
10 compromise (BEC), Distributed Denial-of-Service (DDoS) Attack, Misconfiguration, Phishing, Malware-Non Ransomware, and Data Espionage.

In the embodiment of the present invention, the quantification model comprises at least one of a Bayesian inference model and/or a Monte Carlo Markov Chain (MCMC)
15 model for quantifying cyber risk.

Another aspect of the present invention is a method for cybersecurity risk management that comprises steps of correlating, via a vulnerability prioritisation module, one or more cyber assets, a plurality of cybersecurity vulnerabilities, and threat intelligence
20 related to the cybersecurity vulnerabilities, to determine a vulnerability risk score.

The above step is followed by prioritising one or more cyber risks based on the vulnerability risk score, via the vulnerability prioritisation module.

25 Thereafter, the method includes the step of linking, via a threat analysis module, one or more attack techniques based on the priority of the one or more cyber risks determined by the vulnerability prioritisation module for assessing a security level of a predefined control technique.

The method further includes the step of calculating, via a quantification module, a cyber resiliency based on the vulnerability risk score of the one or more cyber risks, followed by quantifying the one or more cyber risks.

- 5 More specifically, the quantification module is further configured to receive data from both the vulnerability prioritisation module and the threat analysis module to optimise the quantification model, thereby enabling optimal quantification of the one or more cyber risks.
- 10 In the embodiment of the present invention, the method further comprises the step of allowing the vulnerability prioritisation module to receive one or more cyber assets from a database.

- In another embodiment of the present invention, the method comprises the step of
- 15 identifying the one or more cyber assets required to be assessed.

BRIEF DESCRIPTION OF THE DRAWINGS

- The advantages and features of the present invention will become better understood
- 20 with reference to the following detailed description taken in conjunction with the accompanying drawings, in which:

Figure 1 illustrates a schematic representation of a system for cybersecurity risk management, according to various embodiments of the present invention.

25

Figure 2 illustrates a flow chart representing a method for cybersecurity risk management, according to various embodiments of the present invention.

Figure 3 illustrates a schematic representation of the cyber quantification approach of

the quantification module as depicted in Figure 1, according to various embodiments of the present invention.

Like numerals denote like elements throughout the figures.

5

DETAILED DESCRIPTION OF THE INVENTION

The exemplary embodiments described herein detail for illustrative purposes are subjected to many variations. It should be emphasised, however, that the present
10 invention is not limited to as disclosed.

It is understood that various omissions and substitutions of equivalents are contemplated as circumstances may suggest or render expedient, but these are intended to cover the application or implementation without departing from the scope of the
15 present invention.

Specifically, the following terms have the meanings indicated below.

The terms “a” and “an” herein do not denote a limitation of quantity, but rather denote
20 the presence of at least one of the referenced items.

The terms “having”, “comprising”, “including”, and “variations” thereof signify the presence of a component.

25 In an aspect of the present invention, a system and a method for cybersecurity risk management are disclosed.

The inventive aspects of the invention along with various components and engineering involved will now be explained with reference to Figures 1 – 3 herein.

Referring to Figure 1, the system (100) comprises a vulnerability prioritisation module (3) operably configured for, correlating one or more cyber assets (1), 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), and prioritising one or more cyber risks based on the vulnerability risk score (4). The term “cyber asset” refers to any computer hardware, software, network, system, or data that plays a role in the operation and functionality of an information technology IT environment. These assets are integral components of digital systems connected over a network.

10 Cybersecurity vulnerabilities are weaknesses in the systems, networks, applications, or processes of the cyber assets (1) that can be exploited by attackers to compromise the confidentiality, integrity, or availability of information.

In the embodiment of the present invention, the system (100) comprises a database for storing one or more cyber assets (1).

15

In the embodiment of the present invention, the database includes a central repository that has asset and system information such as Configuration Management Databases (CMDB) and Excel files to store information of one or more cyber assets.

20

In the embodiment of the present invention, the Configuration Management Databases (CMDB) may be, but not limited to, ServiceNow and SolarWinds.

In the embodiment of the present invention, the cyber assets (1) and threat intelligence (2a) related to cybersecurity vulnerabilities (2) are gathered from a vast network of sources including, but not limited to, deep and dark web forums, social media platforms, closed-sourced communication channels (e.g., Telegram), code repositories, exploit tool repositories (e.g., Metasploit).

25

More specifically, the sources provide valuable insights into the latest hacking techniques, vulnerabilities, and exploits being used by cybercriminals.

In the embodiment of the present invention, the type of information gathered from the
5 CMDB include, but shall not be limited to, asset type (e.g., hardware, software), application service (e.g., Windows, Unix, etc.), asset owner, department, etc.

Furthermore, the platform is able to use information on the asset such as the system it belongs to, the sensitivity of data it holds, and impact it has on the business to determine
10 the criticality of the asset. At least one or a combination of these information are then used as parameter(s) to calculate vulnerability risk score (4). The said parameter(s) may be quantitative data or variables. With this, it is to be noted that the vulnerability risk score (4) is determined based on three main metrics that include vulnerability severity, threat intelligence (2a), and asset criticality.

15 Moreover, the sources refresh their data in real-time, ensuring that vulnerability risk score (4) and threat assessments are always up-to-date. This dynamic approach allows the system and method as provided by the present invention to stay ahead of the curve, anticipating and mitigating threats before they can materialise into damaging attacks.

20 In the embodiment of the present invention, the vulnerability prioritisation module (3) is operably configured to communicate with the database for receiving the one or more cyber assets (1).

25 Furthermore, the vulnerability prioritisation module (3) utilises artificial intelligence (AI) algorithms to analyse cyber assets (1), extracting key intelligence that is then used to determine vulnerability risk score (4) by calculating it based on vulnerability severity, threat intelligence (2a), and asset criticality. This real-time analysis ensures that the vulnerability risk score (4) remains accurate and reflects the ever-changing threat

landscape. "Key intelligence" refers to crucial information about potential cyber threats, vulnerabilities, or tactics used by malicious actors that is essential to enhance cybersecurity measures and protect the cyber assets (1).

- 5 In the embodiment of the present invention, the plurality of cybersecurity vulnerabilities (2) is identified and evaluated by using Commercial-off-the-shelf (COTS) tools such as, but not limited to, Nessus and Qualys.

More specifically, the system (100) receives the results of cybersecurity vulnerabilities
10 assessment via connectors such as, but not limited to, Application Programming Interface (API).

Moreover, connectors are provided for table-based dataset sources stored in Comma Separated Values (CSV) or Microsoft Excel formats.

15

Additionally, the system (100) receives the results of the cybersecurity vulnerabilities assessment by collecting a large amount of data at once from PDF reports. In this embodiment, the system (100) uses software such as, but not limited to, Amazon Textract Machine Learning (ML).

20

In the embodiment of the present invention, the vulnerability prioritisation module (3) automatically identifies assets based on IP addresses and domain names and extracts the relevant asset parameters from the CMDB in order to generate the vulnerability risk score (4). The said parameters may be quantitative data or variables.

25

Further cybersecurity vulnerabilities (2) are enriched with threat intelligence sources to determine the exploitability, accessibility, and chatter levels.

In an exemplary embodiment of the present invention, the vulnerability prioritisation

module (3) uses seven parameters to calculate a risk score for each vulnerability, the parameters being Dark Web Chatter, the Vulnerability Severity, the Asset Criticality (BIA/CIA), Asset Owner, Asset Identifier (IP address/DNS), Availability of Exploit and Ease of Exploitability. The said parameters may be quantitative data or variables. It is
5 to be noted that the number of parameters may also not be limited to the said number.

More specifically, the higher the vulnerability risk score (4) is, the higher the priority of the vulnerability is. This helps organisations to focus their remediation efforts on the vulnerabilities that pose the greatest risk to their organisation.

10

In another embodiment of the present invention, the system (100) comprises a threat analysis module (11) operably configured to link one or more known or existing 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
15 control technique.

In the embodiment of the present invention, the threat analysis (11) module receives threat intelligence data related to one or more cyber threats and analyses the said data. Furthermore, the threat analysis module (11) filters the threat intelligence based on the
20 results of the vulnerability prioritisation module (3) to identify the only relevant threats to the system. It is to be noted that the threat intelligence data received by the threat analysis module (11) is different from the threat intelligence (2a). More specifically, this threat intelligence data is specific towards operational threat intelligence on past incidents and cyberattacks that have occurred in the threat landscape.

25

More specifically, the cyber threats comprise real-world threats.

In the embodiment of the present invention, 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.

In an exemplary embodiment of the present invention, the system (100) includes a
5 library comprising a comprehensive set of attack scenarios for each real-world threat, which can be used by organisations to test their security defences and identify areas for improvement.

More specifically, the library comprises, but shall not be limited to, Insider Threat,
10 Business Email Compromise (BEC), Distributed Denial-of-Service (DDoS), Malware (Non-Ransomware), Ransomware, Misconfiguration, Data Exfiltration, Supply Chain and Phishing.

In the embodiment of the present invention, the threat analysis module (11) identifies
15 the Tactics, Techniques, and Procedures (TTPs) that are commonly used by attackers in specific threat scenarios.

More specifically, TTPs are the specific methods and tools that attackers use to carry out attacks. Identification of TTPs associated with threat scenarios allows organisations
20 to understand how attackers are likely to attack them and to develop defences to mitigate those risks and prioritise defences that are required to defend against them.

Additionally, the threat analysis module (11) identifies Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) and links security controls for assessing a
25 security level of a predefined control technique.

More specifically, ATT&CK is a framework to describe and categorise the tactics, techniques, and procedures (TTPs) used by attackers during cyberattacks. Moreover, it is a knowledge base of adversary behaviour used by security professionals to

understand and defend against cyberattacks.

ATT&CK techniques comprise at least one of the Initial Access, Persistence, Defence Evasion, Credential Access, Discovery, Command and Control and Exfiltration.

5

Furthermore, the threat analysis module (11) is configured for linking at least one of the ATT&CK techniques to at least one of the security control frameworks defined by, but shall not be limited to, ISO27001:2022, NIST 800-53, NIST Cybersecurity Framework, Cybersafe, and CCOPv2, thereby assessing the strength of the security

10 control frameworks.

In the embodiment of the present invention, the system (100) further comprises a quantification module (12) that comprises a predefined quantification model for calculating cyber resiliency based on the vulnerability risk score (4) of the one or more

15 cyber risks and quantifying the one or more cyber risks.

Further, the quantification module (12) is configured to receive data from both the vulnerability prioritisation module (3) and the threat analysis module (11) to optimise the quantification model, thereby enabling optimal quantification of the one or more

20 cyber risks.

In the embodiment of the present invention, at least one of the threat-based approaches is used to calculate cyber resiliency.

25 In the embodiment of the present invention, the threat-based approach focuses on identifying and mitigating all known cyber threats, regardless of the likelihood of an attack.

In an exemplary embodiment of the present invention, the calculation of cyber

resiliency has been explained by taking the threat category: Ransomware, as an example. However, it should be understood that the calculation of cyber resiliency may involve, shall not be limited to, the threat category: Ransomware.

- 5 In the embodiment of the present invention, there are various variants of ransomware attacks that differ in attack pathways within the threat category: Ransomware.

Here the cyber resiliency is calculated using the below equation:

$$Resiliency = (R1 + R3 + R4 + R8) / 4$$

- 10 wherein,

R1, R2, R3 & R8 = specific variants of ransomware attacks

- More specifically, the above equation takes into account the resilience of the organisation to each of the four ransomware variants (R1, R2, R3 & R8), weighted by
15 the likelihood of an attack from each variant.

Further, the four ransomware variants (R1, R2, R3 & R8) are chosen based on the organisation's profile and threat environment.

- 20 Therefore, the organisation can then use this resiliency to assess its overall risk exposure to ransomware attacks and to identify areas where it can improve its resilience.

- As illustrated in Figure 3, an approach to cyber risk quantification, by quantification model, has been illustrated, for evaluating the potential financial impact of a particular
25 cyber threat.

As illustrated in Figure 3, at least one or both the cyber resiliency (5) and financial data (6) are used by the quantification model to calculate the estimated loss (7) from cyber risk.

Referring to Figure 3, the determination of cyber resiliency (5) includes identifying the cyber threats (9), a plurality of cybersecurity vulnerabilities (2) that could be exploited by the cyber threats (9), and the security controls (10) that are in place to mitigate those risks. Further, the cyber assets (1) are also identified and mapped to the relevant cyber threats (9) and cybersecurity vulnerabilities (2).

Referring to Figure 3, the likelihood and impact of each cyber threat (9) are calculated based on factors such as, but not limited to, the sophistication of the cyber threat (9), the ease of exploitation of the cybersecurity vulnerabilities (2), and the organisation's security controls (10). Additionally, the impact is calculated based on, but shall not be limited to, the potential financial losses, reputational damage, and other negative consequences of a successful cyber attack.

Referring to Figure 3, financial data (6), such as revenue, profits, and assets are identified which is then used to estimate the potential financial impact of a cyberattack. Additionally, the financial data (6) is obtained from sources such as, but not limited to, industry reports and insurance companies.

As illustrated in Figure 3, the quantification model uses advanced risk models (8) to calculate the overall cyber risk exposure of the organisation, based on at least one of the inputs from the cyber resiliency (5) and financial data (6).

Herein, the results of the cyber risk quantification are used to make informed decisions about cyber insurance coverage and cyber investments. This helps the organisation to manage its cyber risk and protect its business.

In another embodiment of the present invention, the quantification model comprises at least one of a Bayesian inference model and/or a Monte Carlo Markov Chain (MCMC)

model for quantifying cyber risk.

More specifically, the Bayesian inference model at least uses any one or a combination of the vulnerability risk scores, cyber loss data, and business impact analysis (BIA) data
5 to calculate a posterior distribution of the Cyber Resiliency Score.

Additionally, the Monte Carlo Markov Chain (MCMC) model uses any one or a combination of the vulnerability risk scores, cyber loss data, and business impact analysis (BIA) data to sample from the posterior distribution of the Cyber Resiliency
10 Score.

Referring now to Figure 2, a method (500) for cybersecurity risk management has been illustrated.

15 As illustrated in Figure 2, the method (500) at step (502) comprises correlating, via a vulnerability prioritisation module (3), one or more cyber assets and a plurality of cybersecurity vulnerabilities, and threat intelligence (2a) related to the cybersecurity vulnerabilities (2), to determine a vulnerability risk score.

20 Further, as illustrated in Figure 2, the method (500) at step (504) includes prioritising, via the vulnerability prioritisation module (3), one or more cyber risks based on the vulnerability risk score.

As illustrated in Figure 2, the above step (504) is followed by step (506) of method
25 (500), which comprises linking, via a threat analysis module (11), one or more known or existing 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.

As illustrated in Figure 2, the method (500) at step (508), comprises calculating, via a quantification module (12), a cyber resiliency based on the vulnerability risk score of the one or more cyber risks followed by step (510) of method (500), quantifying the one or more cyber risks.

5

Whilst not shown, the system (100) may further include at least one computer having at least one processor that is interfaced with the database, and at least one communication unit that enables it to communicate with the database and/or the aforementioned sources in a wired and/or wireless manner.

10

The processor may operate any one or a combination of the vulnerability prioritisation module (3), the threat analysis module (11), and the quantification module (12) based on the descriptions above. It should be noted that while the aforementioned modules may be in a software embodiment, they may also be a hardware embodiment where they are directly connected to the processor. Alternatively, these modules may each be an independent computer system. The processor may be, but shall not be limited to, a conventional processor, an application-specific integrated circuit (ASIC), a field-programmable gate array (FPGA), a graphics processing unit (GPU), or a combination thereof.

15

20

Advantageously, the present invention provides a risk quantification approach that is superior over the other approaches as it is a more data-driven approach to derive underlying distributions of a risk qualification model.

25

Advantageously as well, the present invention takes into account the constantly changing threat landscape within its risk calculations through the ingestion of open vulnerabilities, active threats, and incidents reported on an ongoing basis.

Advantageously as well, the present invention provides a comprehensive end-to-end model of cyber risk and how the cyber risk would materialise in the organisation so that ambiguities in deriving risk and distribution parameters are removed.

- 5 The foregoing descriptions of specific embodiments of the present invention have been presented for purposes of description. They are not intended to be exhaustive or to limit the present invention to the precise forms disclosed, and obviously, many modifications and variations are possible in light of the above teaching.
- 10 Further, the embodiments were chosen and described in order to best explain the principles of the present invention and its practical applications, and thereby enable others skilled in the art to best utilise the present invention and various embodiments with various modifications as are suited to the particular use contemplated.
- 15 It is understood that various omissions and substitutions of equivalents are contemplated as circumstances may suggest or render expedient, but such omissions and substitutions are intended to cover the application or implementation without departing from the scope of the present invention.

20

25

CLAIMS

1. A system for cybersecurity risk management for at least one organisation comprising:
 - 5 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
 - 10 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
 - 15 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
 - 20 (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
 - 25 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
5 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
10 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).

15 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.

20 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.

25 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;

5 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;

10 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

15 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

20

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.

25

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.

- 5 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
- 10 (9),
- wherein the cyber threats (9) comprise real-world threats.

15

20

25