

1. Apparatus for calculating economic loss from electronic threats capable of affecting computer networks, a network includes at least two interconnected networks and at least two IT systems, the threats including at least one electronic threat, and business processes operating on the IT systems, the apparatus including one or more computer processors and a computer readable memory coupled to the one or more computer processors in which programming code is stored, wherein the one or more computer processors are configured pursuant to programming code in the computer readable memory to:

predict for each electronic threat capable of affecting computer networks in which IT systems operate, future threat activity based on past electronic threat activity wherein the electronic threats include computer viruses, Trojan horses, computer worms, malware, malicious signed binaries, hacking, and denial of service attacks, to receive electronic threat data from a database, to extrapolate future electronic threat event frequency and to produce a profile of predicted electronic threat activity comprising a list of predicted electronic threats and their expected frequency of occurrence, wherein the electronic threat data includes observed threats and, for each electronic threat, one or more targets for the electronic threat and a severity score for each target;

determine expected downtime of each system of the IT systems independence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency;

determine economic loss for each of the business processes dependent on the downtimes of the IT systems, and;

add economic losses for each business process to obtain a combined economic loss arising from the electronic threat activity.

2. The apparatus according to claim 1, wherein the instructions comprise:

a first module configured to determine the predicted electronic threat activity, to receive electronic threat data from a database, to extrapolate future event frequency and to produce a profile of predicted electronic threat activity comprising a list of predicted electronic threats and their expected frequency of occurrence, wherein the electronic threat data includes observed threats and, for each electronic threat, one or more targets for the electronic threat and a severity score for each target;

a second module configured to determine the expected downtime of each IT system in dependence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency; and

a third module configured to determine the economic loss for each business process.

3. The apparatus according to claim 2, wherein the third module is configured to add the economic losses for the business processes.

4. The apparatus according to claim 1, wherein the apparatus is further configured to store at least one of the economic losses and the combined economic loss in a storage device.

5. The apparatus according to claim 1, wherein the apparatus is configured to display at least one of the economic losses and the combined economic loss on a display device.

6. The apparatus according to claim 1, further configured to:

retrieve electronic threat data from a database automatically, or in response to user instruction;

determine a time profile in terms of one or more time blocks and the number of successful electronic threats expected in each time block;

receive the number of electronic threats contracted in a given period of time by a network, via an input device from a user;

extrapolate event frequency from historical data using user-editable factors based upon external data sources;

extrapolate future event frequency and produce a profile comprising a list of predicted electronic threats and their expected frequency of occurrence;

and output the predicted electronic threat activity to a firewall to obtain optimum operating performance.

7. The apparatus according to claim 1, wherein loss is expressed as the;

predicted economic loss;

quantified economic loss from disabled business processes;

economic loss value input for business impact analysis;

minimum business interruption insurance cover level required to maintain the same level of production prior to a successful electronic attack;

minimum insurance loss exposure.

8. The apparatus according to claim 1, further configured to output a report of at least one of the predicted economic losses and the combined economic loss.

9. The apparatus according to claim 1, wherein the list of electronic threats includes, for each electronic threat, information identifying at least one IT system.

10. The apparatus according to claim 1, wherein the list of electronic threats includes, for each electronic threat, information identifying frequency of occurrence of the threat.

11. The apparatus according to claim 10, wherein the frequency of occurrence of the electronic threat includes at least one period of time and corresponding frequency of occurrence for the at least one period of time.

12. The apparatus according to claim 1 wherein the IT systems include software systems, hardware systems, or a combination thereof.

13. A method for calculating economic loss from electronic threats capable of affecting computer networks, a network includes at least two interconnected networks and at least two IT systems, the threats including at least one electronic threat, and business processes operating on the IT systems, the apparatus including one or more computer processors and a computer readable memory coupled to the one or more computer processors in which programming code is stored, wherein the one or more computer processors are configured pursuant to programming code in the computer readable memory to:

predict for each electronic threat capable of affecting computer networks in which IT systems operate, future threat activity based on past electronic threat activity wherein the electronic threats include computer viruses, Trojan horses, computer worms, malware, malicious signed binaries, hacking, and denial of service attacks, to receive electronic threat data from a database, to extrapolate future electronic threat event frequency and to produce a profile of predicted electronic threat activity comprising a list of predicted threats and their expected frequency of occurrence, wherein the electronic threat data includes observed threats and, for each electronic threat, one or more targets for the electronic threat and a severity score for each target;

determine expected downtime of each system of the IT systems independence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency;

determine economic loss for each of the business processes dependent on the downtimes of the IT systems, and;

add economic losses for the business processes to obtain a combined economic loss arising from the threat activity.

14. The method according to claim 13, further comprising:
storing at least one of the economic losses and combined economic loss in a storage device.
15. The method according to claim 13, further comprising:
displaying at least one of the economic losses and combined economic loss on a display device.
16. A computer readable memory storing a computer program which when executed by a computer system, causes the computer system to perform a method of calculating economic loss from electronic threats capable of affecting computer networks, the computer network comprising IT systems, wherein business processes operate on the IT systems, the method comprising:

predicting future electronic threat activity based on historical electronic threat activity, for each electronic threat capable of affecting computer networks in which IT systems operate;

to receive electronic threat data from a database, to extrapolate future electronic threat event frequency and to produce a profile of predicted electronic threat activity comprising a list of predicted electronic threats and their expected frequency of occurrence, wherein the electronic threat data includes observed threats and, for each

electronic threat, one or more targets for the electronic threat and a severity score for each target;

determining expected downtime of each system of the total IT systems in dependence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency;

determining economic loss for each of the business processes dependent on the downtimes of the IT systems, and;

adding economic losses for each business process to obtain a combined economic loss arising from the electronic threat activity.