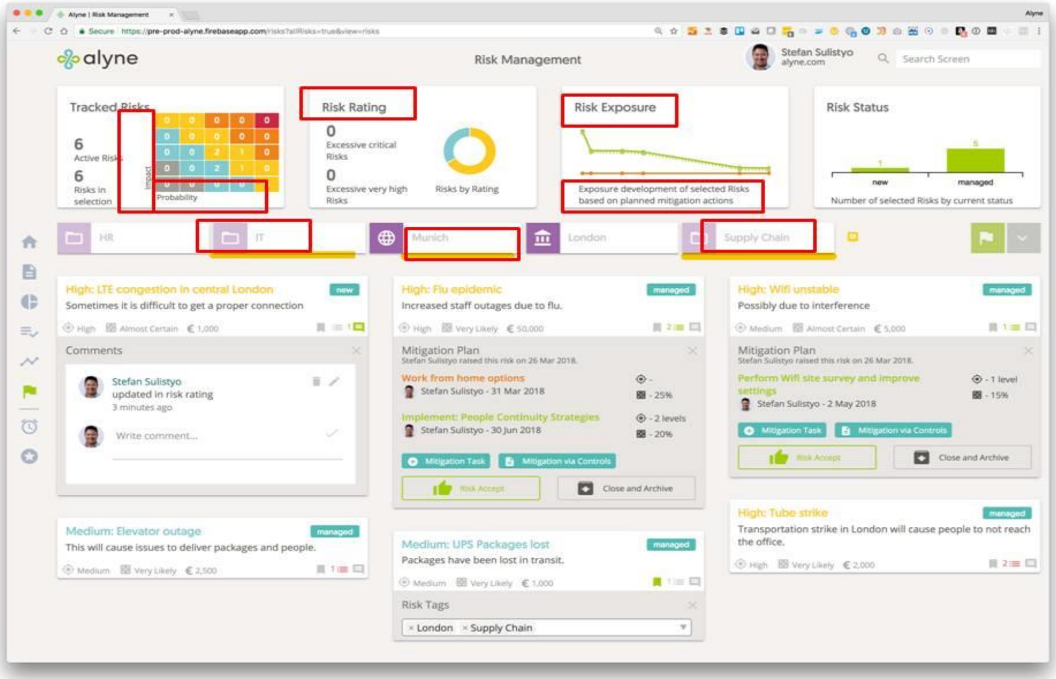
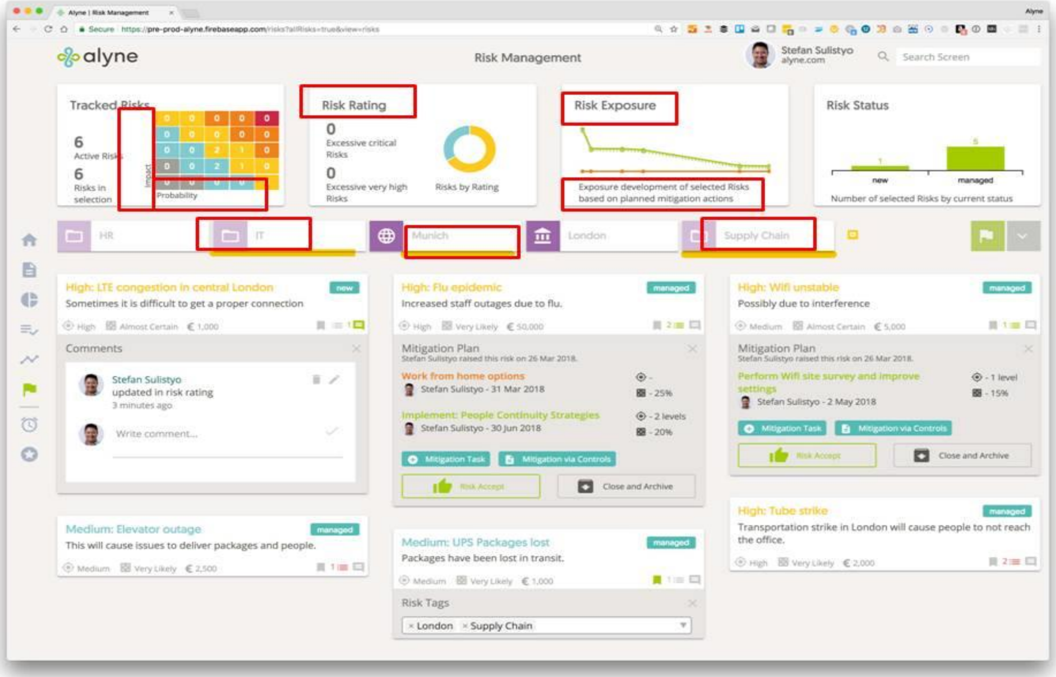
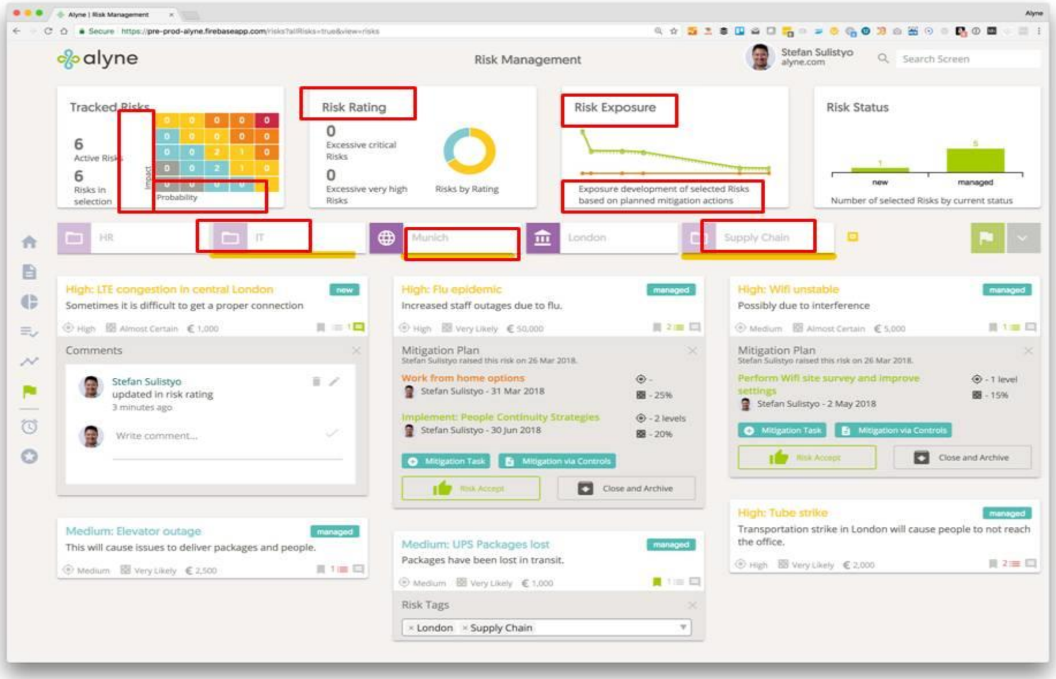
# ALYNE

| EXHIBIT A | |
|---|---|
| **Quantar's Preliminary Infringement Contentions** | |
| **US Patent No: 9143523 12/811,208** | **Accused Instrumentalities** |
| **Claim: 1** | |
| 1. Apparatus for assessing threat to at least one computer network, the threat including at least one electronic threat, the computer network comprising a plurality of IT systems and a plurality of business processes operating on the plurality of IT systems, wherein (a) at least one IT system has two or more of the plurality of business processes operating thereon or (b) at least one business process operates on two or more of the plurality of IT systems, the apparatus comprising at least one processor and a memory coupled to the processor, the memory storing instructions executable by the processor that cause the processor to: | |
| | |

| | |
|---|---|
| predict future threat activity based on past observed threat activity including, for the at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target, determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency, determine loss for each of the plurality of business processes dependent on the downtimes of the IT systems, and add losses for the plurality of business processes so as to obtain a combined loss arising from the threat activity. | ALYNE 2;<br><br> Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>Alyne<br>alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6<br>Active Risks<br>6<br>Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1<br>5<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London<br>new<br>Sometimes it is difficult to get a proper connection<br>High Almost Certain € 1,000<br>Comments<br>Stefan Sulistyo<br>updated in risk rating<br>3 minutes ago<br>Write comment...<br>Medium: Elevator outage<br>managed<br>This will cause issues to deliver packages and people.<br>Medium Very Likely € 2,500<br>High: Flu epidemic<br>managed<br>Increased staff outages due to flu.<br>High Very Likely € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018<br>- <br>- 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018<br>- 2 levels<br>- 20%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost<br>managed<br>Packages have been lost in transit.<br>Medium Very Likely € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable<br>managed<br>Possibly due to interference<br>Medium Almost Certain € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018<br>- 1 level<br>- 15%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike<br>managed<br>Transportation strike in London will cause people to not reach the office.<br>High Very Likely € 2,000 |
| **Claim: 12** | |
| 12. A method of assessing threat to at least one computer network, the threat including at least one electronic threat, the network comprising a plurality of IT systems wherein a plurality of business processes operate on the plurality of IT systems, and wherein (a) at least one IT system has two or more of the plurality of business processes operating thereon or (b) at least one business process operates on two or more of the plurality of IT systems, the method comprising, by using at least one computer processor: | |

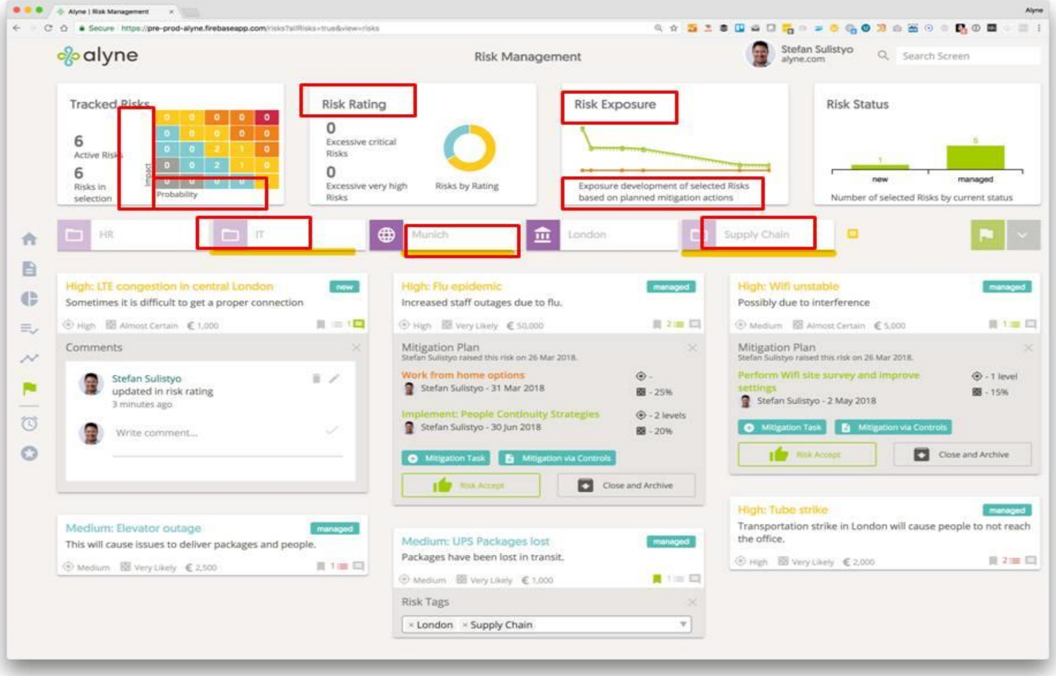
| | |
|---|---|
| predicting threat activity based on past observed activity including, for the at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |
| determining expected downtime of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018 · - · - 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018 · - 2 levels · - 20%<br>Mitigation Task · Mitigation via Controls<br>Risk Accept · Close and Archive<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018 · - 1 level · - 15%<br>Mitigation Task · Mitigation via Controls<br>Risk Accept · Close and Archive<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 |
| determining loss for the plurality of business processes dependent on the downtimes of the IT systems; | |

| | |
|---|---|
| adding losses for the plurality of business processes to obtain a combined loss arising from the threat activity. | |
| **Claim: 15** | |
| 15. A non-transitory computer readable medium storing a computer program which when executed by a computer system, causes the computer system to perform a method of assessing threat to at least one computer network, the threat including at least one electronic threat, the computer network comprising a plurality of IT systems wherein a plurality of business processes operate on the plurality of IT systems, and wherein (a) at least one IT system has two or more of the plurality of business processes operating thereon or (b) at least one business process operates on two or more of the plurality of IT systems, the method comprising: | |
| predicting threat activity based on past observed activity including, for the at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |

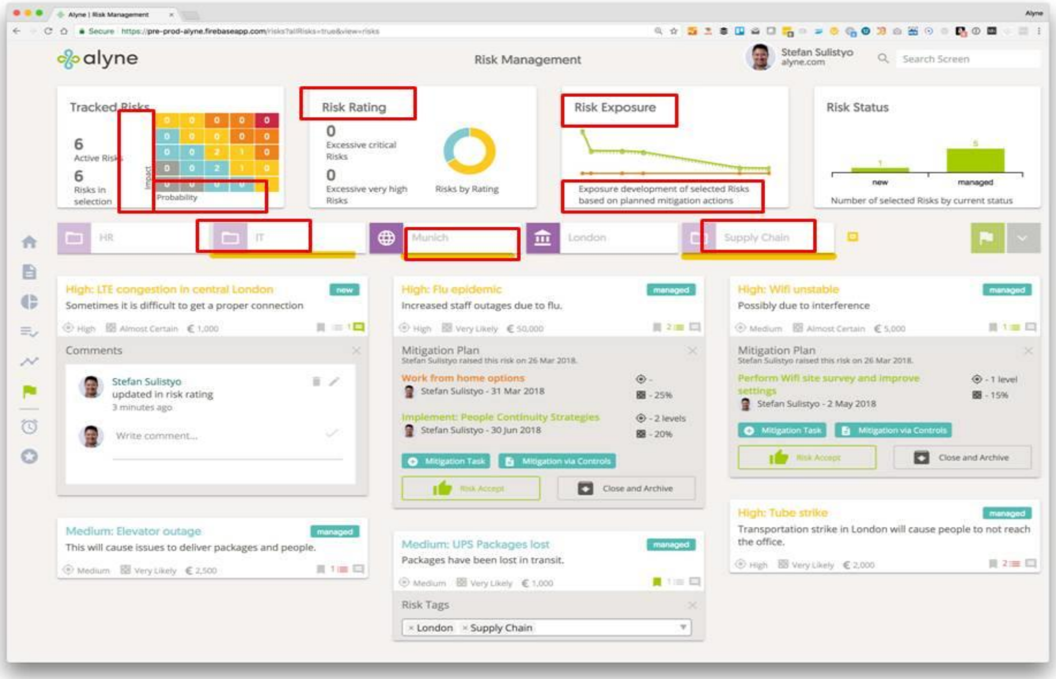
| | |
|---|---|
| determining expected downtime of each of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018 · - · - 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018 · - 2 levels · - 20%<br>Mitigation Task · Mitigation via Controls · Risk Accept · Close and Archive<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018 · - 1 level · - 15%<br>Mitigation Task · Mitigation via Controls · Risk Accept · Close and Archive<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 |
| determining loss for the plurality of business processes dependent on the downtimes of the IT systems; | |
| adding losses for the plurality of business processes to obtain a combined loss arising from the threat activity. | |

**Note:** Total claims: 15 and Independent claims: 3

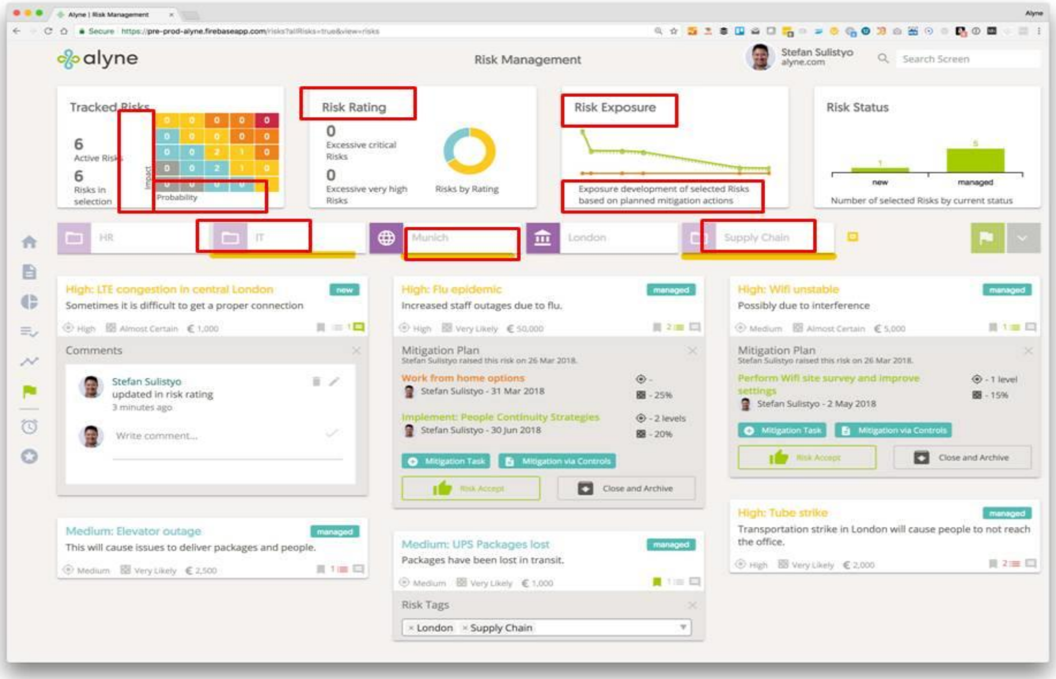
| EXHIBIT B | |
|---|---|
| Quantar’s Preliminary Infringement Contentions | |
| US Patent No: 9363279 13/322,298 | Accused Instrumentalities |
| Claim: 1 | |
| 1. An apparatus including one or more computer processors and a non-transient computer readable memory, wherein the one or more computer processors are configured pursuant to programming code in a the non-transient computer readable memory to predict, for each of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity using a Monte Carlo method based on stochastic modelling of past observed threat events, wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses, wherein the one or more computer processors are configured, for a given threat, to model a set of past observed threat events to obtain an estimate of at least one model parameter, and, in a Monte Carlo simulation of a given threat, to predict future threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable, and to predict a distribution of future threat | |

| | |
|---|---|
| events by repeating the simulation using a plurality of variables; and | |
| | |
| wherein the apparatus is further configured to determine an expected downtime of each of said systems in dependence upon said predicted future threat activity and to determine a financial loss for each of a plurality of operational processes dependent on the downtimes of each of said systems and to add the financial losses for said plurality of processes so as to obtain a combined financial loss arising from the predicted future threat activity. | ALYNE 2;<br><br> Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>Alyne<br>alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6<br>Active Risks<br>6<br>Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1<br>5<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High — Almost Certain — € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium — Very Likely — € 2,500<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High — Very Likely — € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - ; - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels ; - 20%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium — Very Likely — € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium — Almost Certain — € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level ; - 15%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High — Very Likely — € 2,000 |
| **Claim: 25** | |
| 25. A computer-implemented method, the method being performed by a computer system having one or more computer processors and a non-transient computer readable memory, the one or more computer processors being configured pursuant to | |

| | |
|---|---|
| programming code in the non-transient computer readable memory, the method comprising: | |
| predicting, for each of a plurality of threats, future threat activity using a Monte Carlo method based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate, wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses; | |
| wherein for each given threat the method comprises: | |
| modelling a set of past observed threat events to obtain an estimate of at least one model parameter; | |
| performing a Monte Carlo simulation of the given threat by: | |
| predicting future threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable, and predicting a distribution of future threat events by repeating the simulation using a plurality of variables; and | |
| | |

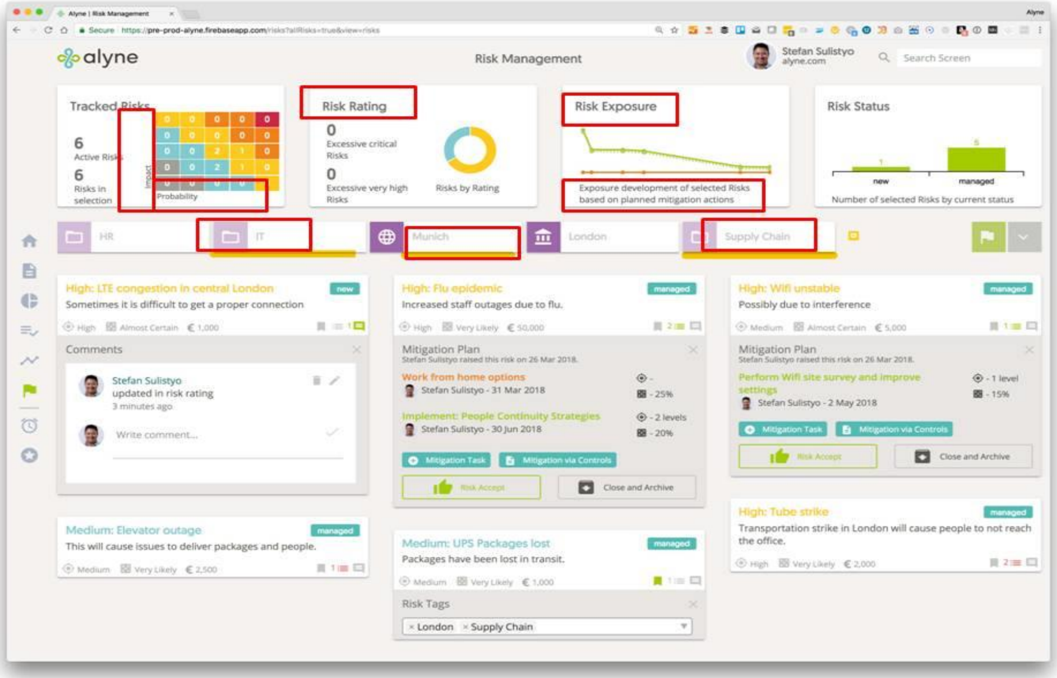
<table>
<tr><td>wherein determining an expected downtime of each system in dependence upon said predicted future threat activity;</td><td>ALYNE 2;<br><br>Alyne &#124; Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1 new<br>5 managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High — Almost Certain — € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium — Very Likely — € 2,500<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High — Very Likely — € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018 — - / - 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018 — - 2 levels / - 20%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium — Very Likely — € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium — Almost Certain — € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018 — - 1 level / - 15%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High — Very Likely — € 2,000</td></tr>
<tr><td>determining a financial loss for each of a plurality of operational processes dependent on the downtimes of the systems;</td><td></td></tr>
<tr><td>adding the financial losses for the plurality of processes to obtain a combined financial loss arising from the future threat activity.</td><td></td></tr>
<tr><td><b>Claim: 29</b></td><td></td></tr>
<tr><td>29. A non-transitory computer readable medium having a computer program thereon, which when executed by a computer system having one or more</td><td></td></tr>
</table>

| | |
|---|---|
| computer processors and a non-transient computer readable memory, causes the computer system to predict, for each of a plurality of threats, future threat activity a Monte Carlo method based on stochastic modelling of past observed threat events capable of affecting at least one computer network in which a plurality of systems operate, wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses; | |
| wherein execution of the computer program causes the computer system to perform, for each given threat, steps comprising: | |
| modelling a set of past observed threat events to obtain an estimate of at least one model parameter; | |
| performing a Monte Carlo simulation of the given threat by: | |
| predicting future threat events using the at least one model parameter and a stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable, and predicting a distribution of future threat events by repeating the simulation using a plurality of variables; and | |
| | |

| | |
|---|---|
| wherein determining an expected downtime of each system in dependence upon said predicted future threat activity; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks: 6 Active Risks; 6 Risks in selection<br>Risk Rating: 0 Excessive critical Risks; 0 Excessive very high Risks; Risks by Rating<br>Risk Exposure: Exposure development of selected Risks based on planned mitigation actions<br>Risk Status: Number of selected Risks by current status<br>HR · IT · Munich · London · Supply Chain<br>High: LTE congestion in central London (new)<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage (managed)<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>High: Flu epidemic (managed)<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options: Stefan Sulistyo - 31 Mar 2018 (- ; - 25%)<br>Implement: People Continuity Strategies: Stefan Sulistyo - 30 Jun 2018 (- 2 levels; - 20%)<br>Medium: UPS Packages lost (managed)<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags: × London × Supply Chain<br>High: Wifi unstable (managed)<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings: Stefan Sulistyo - 2 May 2018 (- 1 level; - 15%)<br>High: Tube strike (managed)<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000<br> alyne<br>Alyne<br>Impact<br>Probability<br>new<br>managed<br>1<br>5<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive |
| determining a financial loss for each of a plurality of operational processes dependent on the downtimes of the systems; | |
| adding the financial losses for the plurality of processes to obtain a combined financial loss arising from the future threat activity. | |

**Note:** Total claims: 30 and Independent claims: 3

| EXHIBIT C | |
|---|---|
| Quantar’s Preliminary Infringement Contentions | |
| US Patent No: 9288224 14/827,712 | Accused Instrumentalities |
| Claim: 1 | |
| 1. Apparatus for assessing and valuing computer network threats, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems and a plurality of business processes operating on the plurality of IT systems, the apparatus comprising at least one processor and a memory coupled to the processor, the memory storing instructions executable by the processor that cause the processor to: | |
| predict future threat activity based on past observed threat activity including, at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |

| | |
|---|---|
| determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br> |
| determine the financial loss for each of the plurality of business processes dependent on the downtimes of the IT systems, and; | |
| add the financial losses for the plurality of business processes so as to obtain a combined financial loss arising from the threat activity. | |
| **Claim: 13** | |
| 13. A method of assessing and valuing computer network threats, the threats including at least one electronic threat, the network comprising a plurality | |

Alyne | Risk Management

https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks

alyne

Risk Management

Stefan Sulistyo
alyne.com

Search Screen

Tracked Risks

6 Active Risks

6 Risks in selection

Risk Rating

0 Excessive critical Risks

0 Excessive very high Risks

Risks by Rating

Risk Exposure

Exposure development of selected Risks based on planned mitigation actions

Risk Status

Number of selected Risks by current status

HR | IT | Munich | London | Supply Chain

High: LTE congestion in central London — new

Sometimes it is difficult to get a proper connection

High | Almost Certain | € 1,000

Comments

Stefan Sulistyo updated in risk rating 3 minutes ago

Write comment...

Medium: Elevator outage — managed

This will cause issues to deliver packages and people.

Medium | Very Likely | € 2,500

High: Flu epidemic — managed

Increased staff outages due to flu.

High | Very Likely | € 50,000

Mitigation Plan

Stefan Sulistyo raised this risk on 26 Mar 2018.

Work from home options — Stefan Sulistyo - 31 Mar 2018 — - | - 25%

Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels | - 20%

Mitigation Task | Mitigation via Controls | Risk Accept | Close and Archive

Medium: UPS Packages lost — managed

Packages have been lost in transit.

Medium | Very Likely | € 1,000

Risk Tags

× London × Supply Chain

High: Wifi unstable — managed

Possibly due to interference

Medium | Almost Certain | € 5,000

Mitigation Plan

Stefan Sulistyo raised this risk on 26 Mar 2018.

Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level | - 15%

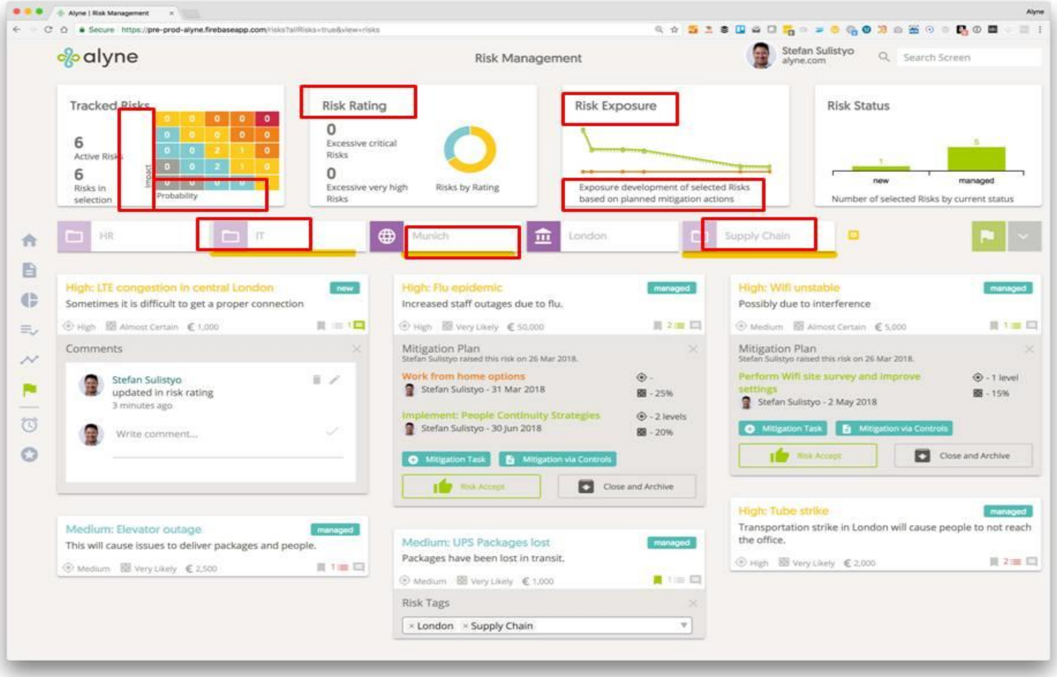
Mitigation Task | Mitigation via Controls | Risk Accept | Close and Archive

High: Tube strike — managed

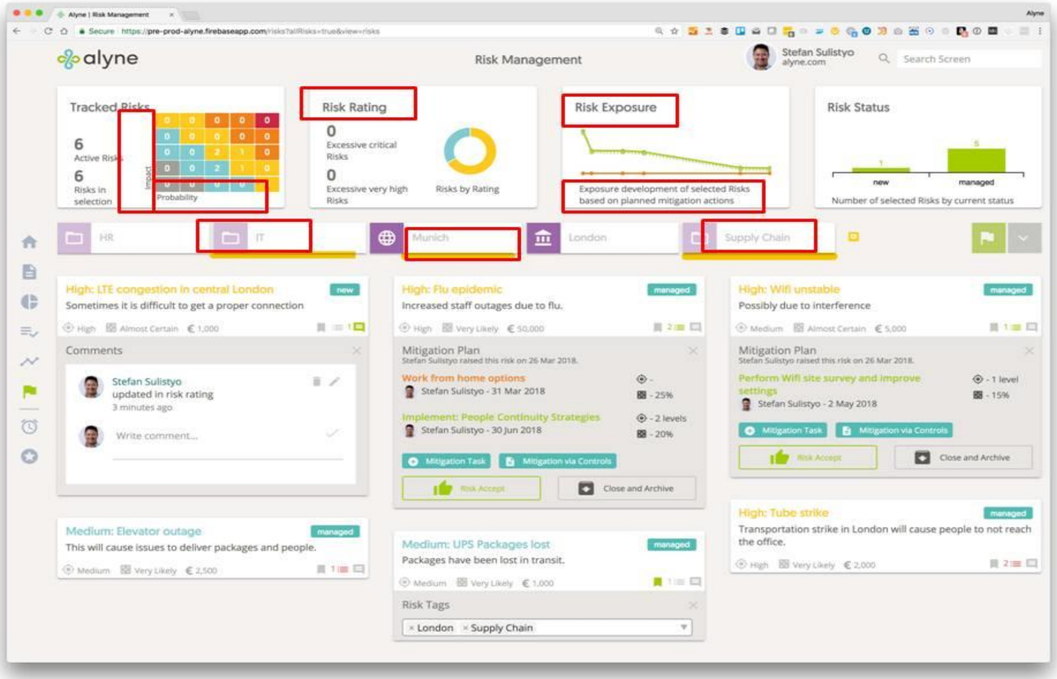
Transportation strike in London will cause people to not reach the office.

High | Very Likely | € 2,000

| | |
|---|---|
| of IT systems wherein a plurality of business processes operate on the plurality of IT systems the method comprising, by using at least one computer processor: | |
| predicting threat activity based on past observed activity including, for at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |

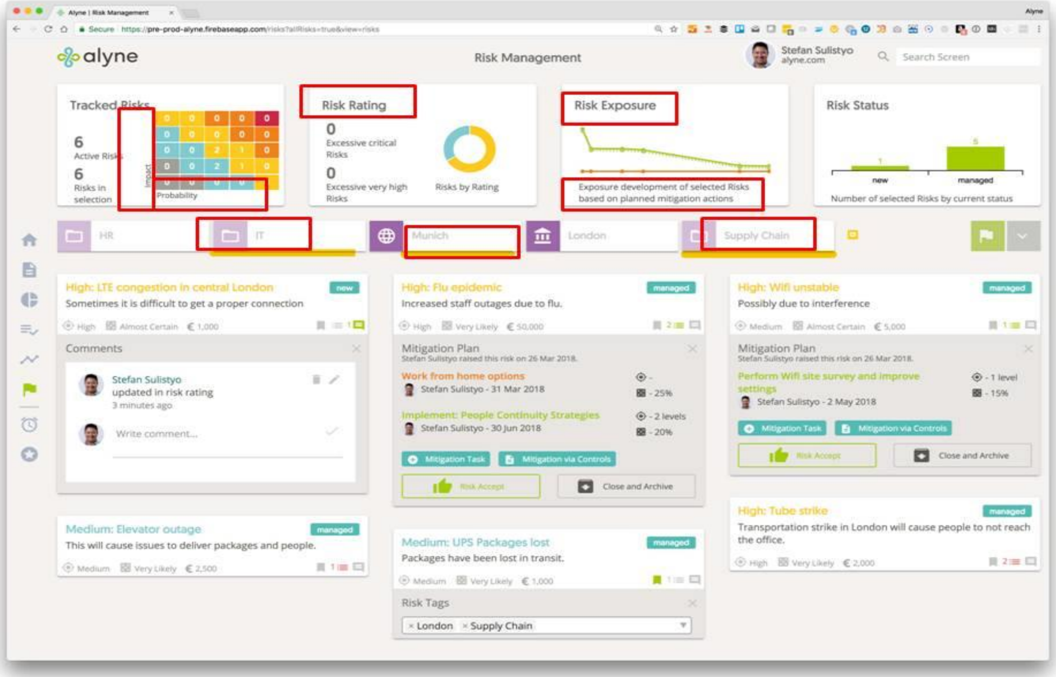
| | |
|---|---|
| determining expected downtime of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br> Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6<br>Active Risks<br>6<br>Risks in selection<br>Impact<br>Probability<br>0 0 0 0 0<br>0 0 0 0 0<br>0 0 2 1 0<br>0 0 2 1 0<br>0 0 0 0<br>Risk Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1<br>5<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000 · 1<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500 · 1<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000 · 2<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - · - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels · - 20%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000 · 1<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000 · 1<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level · - 15%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 · 2 |
| determining the financial loss for the plurality of business processes dependent on the downtimes of the IT systems; | |
| adding the financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity. | |
| **Claim: 16** | |
| 16. A non-transitory computer readable medium storing a computer program which when executed by a computer system, causes the computer system | |

| | |
|---|---|
| to perform a method of assessing and valuing computer network threats, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems wherein a plurality of business processes operate on the plurality of IT systems, the method comprising: | |
| predicting threat activity based on past observed activity including, at least one electronic threat, to receive observed threat data from a database, to extrapolate future event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |

| | |
|---|---|
| determining expected downtime of each of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Tracked Risks: 6 Active Risks; 6 Risks in selection<br>Risk Rating: 0 Excessive critical Risks; 0 Excessive very high Risks; Risks by Rating<br>Risk Exposure: Exposure development of selected Risks based on planned mitigation actions<br>Risk Status: new 1; managed 5; Number of selected Risks by current status<br>HR; IT; Munich; London; Supply Chain<br>High: LTE congestion in central London (new) – Sometimes it is difficult to get a proper connection – High, Almost Certain, € 1,000<br>Comments: Stefan Sulistyo updated in risk rating 3 minutes ago; Write comment...<br>Medium: Elevator outage (managed) – This will cause issues to deliver packages and people. – Medium, Very Likely, € 2,500<br>High: Flu epidemic (managed) – Increased staff outages due to flu. – High, Very Likely, € 50,000<br>Mitigation Plan: Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options – Stefan Sulistyo - 31 Mar 2018 – - ; - 25%<br>Implement: People Continuity Strategies – Stefan Sulistyo - 30 Jun 2018 – - 2 levels; - 20%<br>Medium: UPS Packages lost (managed) – Packages have been lost in transit. – Medium, Very Likely, € 1,000<br>Risk Tags: London, Supply Chain<br>High: Wifi unstable (managed) – Possibly due to interference – Medium, Almost Certain, € 5,000<br>Mitigation Plan: Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings – Stefan Sulistyo - 2 May 2018 – - 1 level; - 15%<br>High: Tube strike (managed) – Transportation strike in London will cause people to not reach the office. – High, Very Likely, € 2,000<br> alyne<br>Search Screen<br>Impact<br>Probability<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Alyne |
| determining the financial loss for the plurality of business processes dependent on the downtimes of the IT systems; | |
| adding the financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity. | |

**Note:** Total claims: 16 and Independent claims: 3

| EXHIBIT D | |
|---|---|
| **Quantar's Preliminary Infringement Contentions** | |
| **US Patent No: 9418226 15/017,645** | **Accused Instrumentalities** |
| **Claim: 1** | |
| 1. Apparatus for assessing financial loss from threats capable of affecting at least one computer network, a network includes a plurality of interconnected networks, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems, an IT system defined in terms of physical location, and a plurality of operational business processes operating on the plurality of IT systems, the apparatus including one or more computer processors and a computer readable memory 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 of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity based on past observed threat activity wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of | |

| | |
|---|---|
| computer viruses, Trojan horses, computer worms, hacking and denial of service attacks, to receive observed threat data from a database, to extrapolate future threat event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |
| determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br> |

Alyne | Risk Management

https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks

Stefan Sulistyo alyne.com

6 Active Risks

6 Risks in selection

0 Excessive critical Risks

0 Excessive very high Risks

Exposure development of selected Risks based on planned mitigation actions

Number of selected Risks by current status

High: LTE congestion in central London — new

Sometimes it is difficult to get a proper connection

High · Almost Certain · € 1,000

Comments

Stefan Sulistyo updated in risk rating 3 minutes ago

Write comment...

Medium: Elevator outage — managed

This will cause issues to deliver packages and people.

Medium · Very Likely · € 2,500

High: Flu epidemic — managed

Increased staff outages due to flu.

High · Very Likely · € 50,000

Mitigation Plan

Stefan Sulistyo raised this risk on 26 Mar 2018.

Work from home options — Stefan Sulistyo - 31 Mar 2018 — - / - 25%

Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels / - 20%

Medium: UPS Packages lost — managed

Packages have been lost in transit.

Medium · Very Likely · € 1,000

Risk Tags: × London × Supply Chain

High: Wifi unstable — managed

Possibly due to interference

Medium · Almost Certain · € 5,000

Mitigation Plan

Stefan Sulistyo raised this risk on 26 Mar 2018.

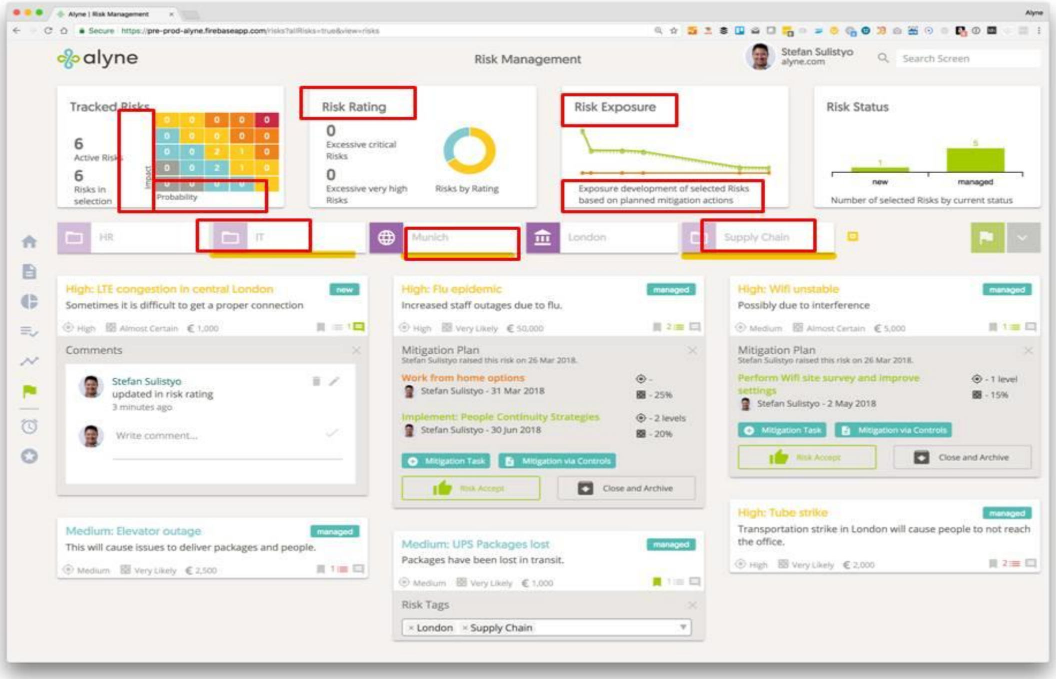
Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level / - 15%

High: Tube strike — managed

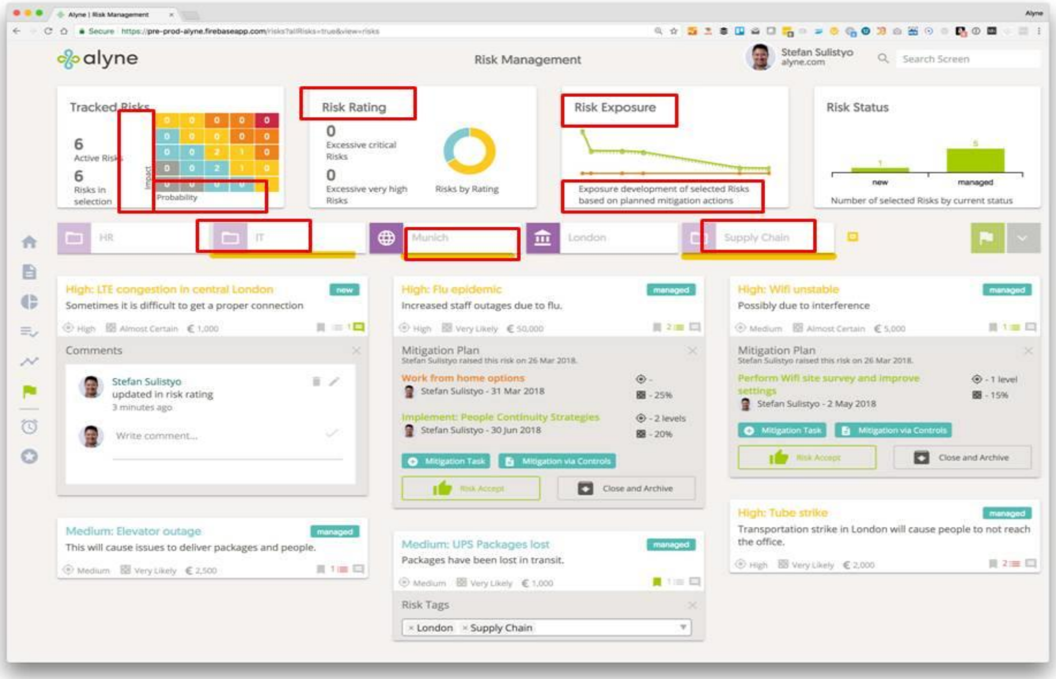
Transportation strike in London will cause people to not reach the office.

High · Very Likely · € 2,000

| | |
|---|---|
| determine financial loss for each of the plurality of operational business processes dependent on the downtimes of the IT systems; | |
| add financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity. | |
| **Claim: 13** | |
| 13. A method for assessing financial loss from threats capable of affecting at least one computer network, a network includes a plurality of interconnected networks, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems, an IT system defined in terms of physical location, and a plurality of operational business processes operating on the plurality of IT systems, the apparatus including one or more computer processors and a computer readable memory 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 of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity based on past observed threat activity wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses, Trojan horses, computer worms, hacking and denial of service attacks, to receive observed threat data from a database, to extrapolate future threat event frequency and to produce a profile of predicted threat activity, wherein the observed | |

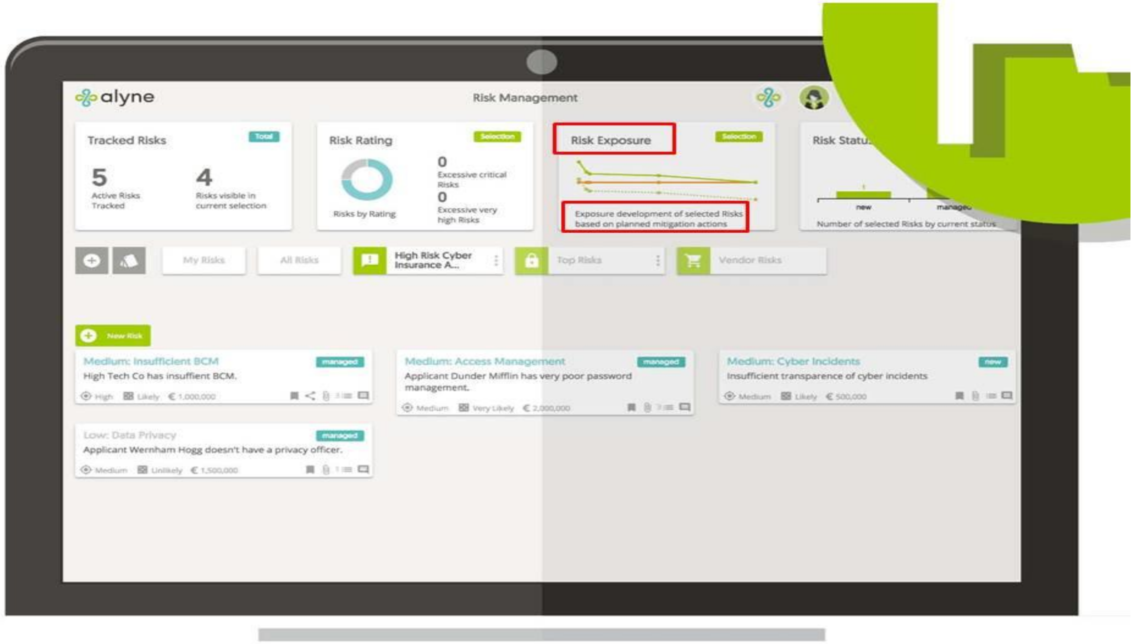
| | |
|---|---|
| threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |
| determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6<br>Active Risks<br>6<br>Risks in selection<br>0 0 0 0 0<br>0 0 0 0 0<br>0 0 2 1 0<br>0 0 2 1 0<br>0 0 0 0<br>Impact<br>Probability<br>Risk Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1<br>5<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London<br>new<br>Sometimes it is difficult to get a proper connection<br>High Almost Certain € 1,000 1<br>Comments<br>Stefan Sulistyo<br>updated in risk rating<br>3 minutes ago<br>Write comment...<br>Medium: Elevator outage<br>managed<br>This will cause issues to deliver packages and people.<br>Medium Very Likely € 2,500 1<br>High: Flu epidemic<br>managed<br>Increased staff outages due to flu.<br>High Very Likely € 50,000 2<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018<br>- <br>- 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018<br>- 2 levels<br>- 20%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost<br>managed<br>Packages have been lost in transit.<br>Medium Very Likely € 1,000 1<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable<br>managed<br>Possibly due to interference<br>Medium Almost Certain € 5,000 1<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018<br>- 1 level<br>- 15%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike<br>managed<br>Transportation strike in London will cause people to not reach the office.<br>High Very Likely € 2,000 2 |
| determine financial loss for each of the plurality of operational business processes dependent on the downtimes of the IT systems; | |
| add financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity. | |

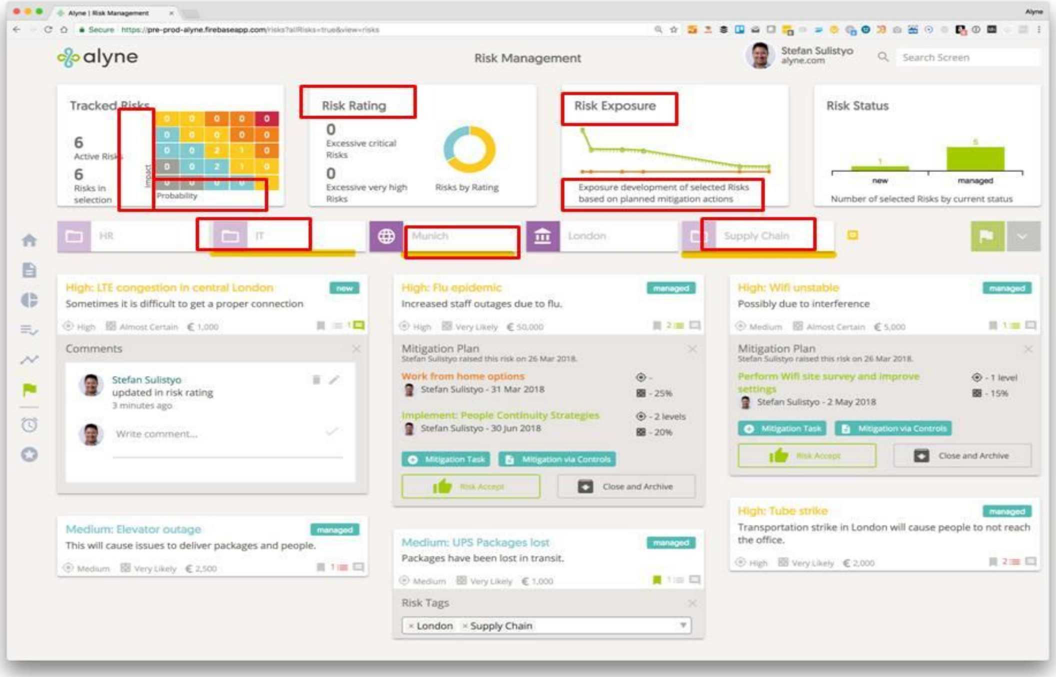
| **Claim: 16** | |
|---|---|
| 16. A non-transitory computer readable memory storing a computer program which when executed by a computer system, causes the computer system to perform a method of assessing financial loss from threats capable of affecting at least one computer network, a network include a plurality of interconnected networks, the threats including at least one electronic threat, the computer network comprising a plurality of IT systems, an IT system defined in terms of physical location, and a plurality of operational business processes operating on the plurality of IT systems, the method comprising: | |
| predict for each of a plurality of threats capable of affecting at least one computer network in which a plurality of systems operate, future threat activity based on past observed threat activity wherein the plurality of threats includes a plurality of electronic threats and the plurality of electronic threats includes a plurality of computer viruses, Trojan horses, computer worms, hacking and denial of service attacks, to receive observed threat data from a database, to extrapolate future threat event frequency and to produce a profile of predicted threat activity, wherein the observed threat data includes observed threats and, for each observed threat, one or more targets for the observed threat and a severity score for each target; | |
| | |

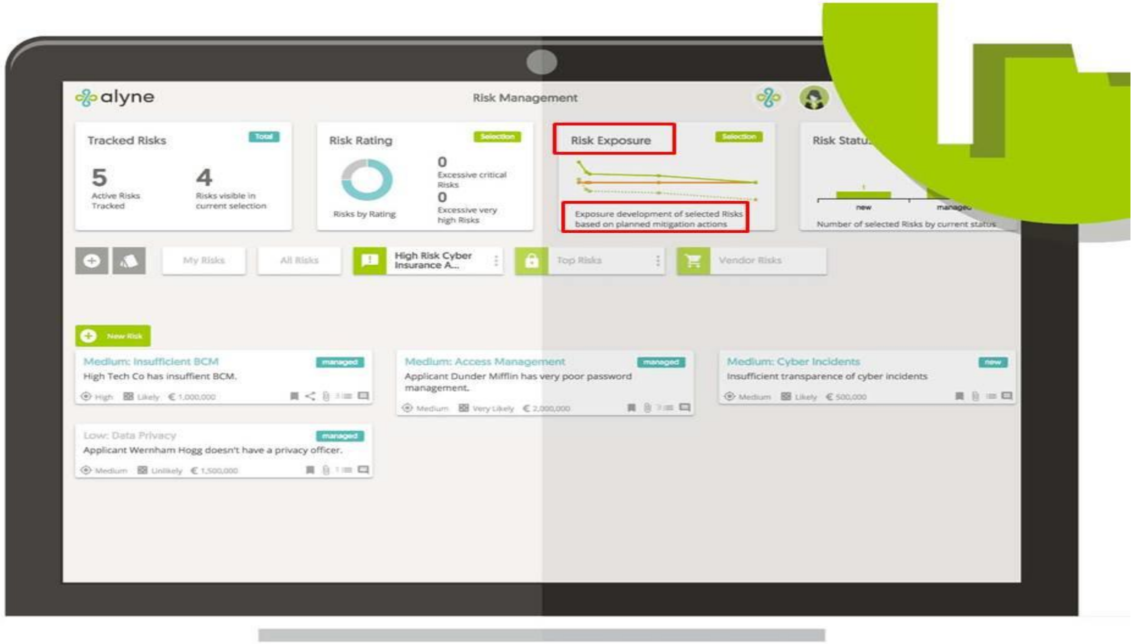
| | |
|---|---|
| determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London new<br>Sometimes it is difficult to get a proper connection<br>High Almost Certain € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage managed<br>This will cause issues to deliver packages and people.<br>Medium Very Likely € 2,500<br>High: Flu epidemic managed<br>Increased staff outages due to flu.<br>High Very Likely € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018<br>- <br>- 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018<br>- 2 levels<br>- 20%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost managed<br>Packages have been lost in transit.<br>Medium Very Likely € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable managed<br>Possibly due to interference<br>Medium Almost Certain € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018<br>- 1 level<br>- 15%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike managed<br>Transportation strike in London will cause people to not reach the office.<br>High Very Likely € 2,000 |
| determine financial loss for each of the plurality of operational business processes dependent on the downtimes of the IT systems; | |
| add financial losses for the plurality of business processes to obtain a combined financial loss arising from the threat activity. | |

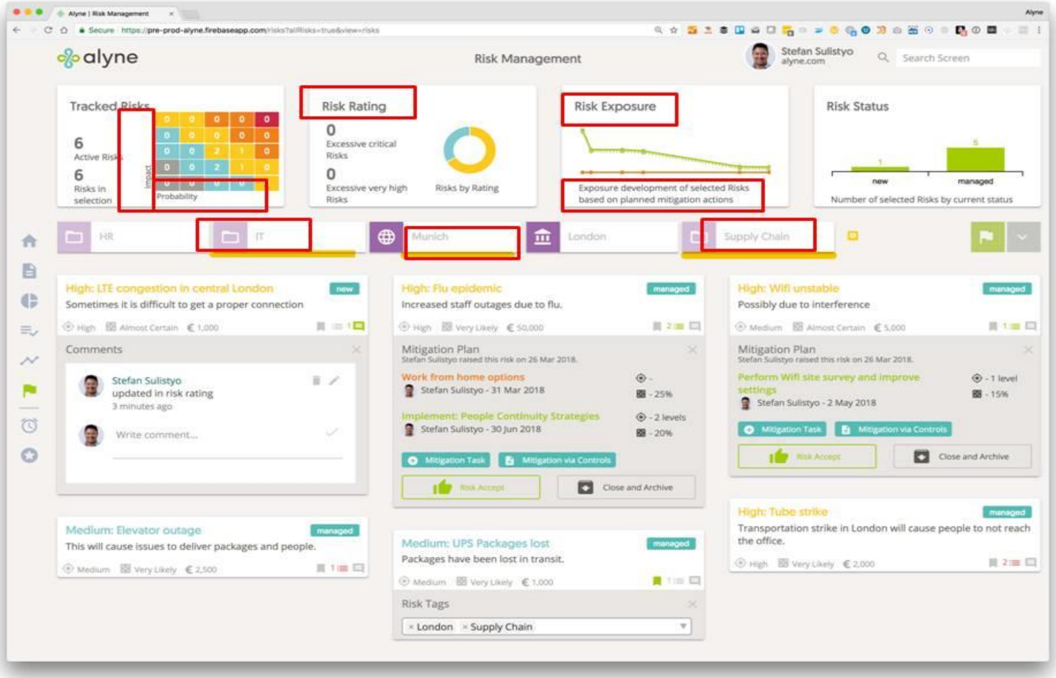
**Note:** Total claims: 16 and Independent claims: 3

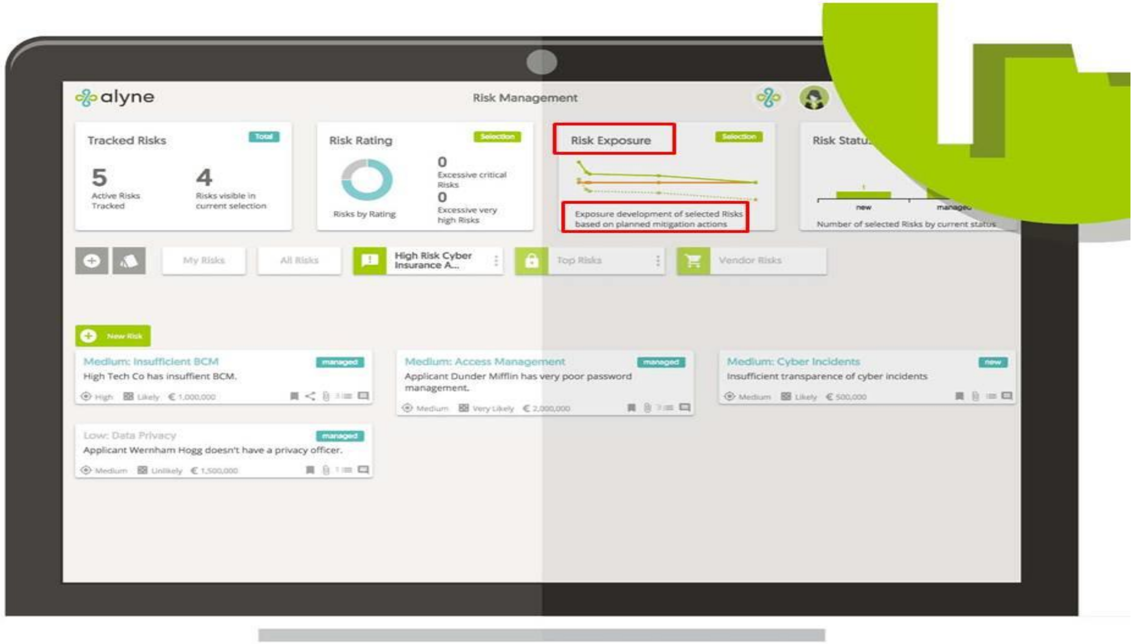
| EXHIBIT E | |
|---|---|
| **Quantar's Preliminary Infringement Contentions** | |
| **US Patent No: 9762605 15/012,182** | **Accused Instrumentalities** |
| **Claim: 1** | |
| 1. Apparatus for assessing financial loss from cyber threats capable of affecting at least one computer network, the threat including at least one electronic threat, the computer network comprising a plurality of IT systems and a plurality of business processes operating on the plurality of IT systems, the apparatus comprising at least one processor configured pursuant to programming code in a non-transitory computer readable memory coupled to the processor, the non-transitory computer memory storing instructions executable by the processor that cause the processor to: | |
| | |

| | |
|---|---|
| predict future cyber threat activity using a Monte Carlo method based on stochastic modeling of actual past observed computer network cyber threat activity, to receive observed cyber threat data from a database, the list of observed cyber threats including information, for each threat, of identification of at least one computer system targeted, to extrapolate future event frequency, to produce a profile of predicted cyber threat activity, wherein for each actual observed cyber threat on the computer network, an identifier, a name, a description of the threat, a temporal profile specifying frequency of occurrence, a target (or targets) for the threat and a severity score for the (each target) are included in the cyber threat data within the database, output the predicted future threat activity to one or more firewalls to improve their accuracy in correctly identifying cyber threats actually observed on the one or more computer networks to improve the accuracy of the apparatus and stochastic modeling of assessing financial loss from cyber threats on an ongoing basis, determine expected downtime of each system of the plurality of IT systems in dependence upon said predicted threat activity including the severity scores and extrapolated future event frequency, determine loss for each of the plurality of business processes dependent on the downtimes of the IT systems, and add losses for the plurality of business processes so as to obtain a combined financial loss arising from the cyber threat activity. | ALYNE 1;<br><br>Medium: Insufficient BCM — High Tech Co has insuffient BCM.<br>Medium: Access Management — Applicant Dunder Mifflin has very poor password management.<br>Medium: Cyber Incidents — Insufficient transparence of cyber incidents<br>Low: Data Privacy — Applicant Wernham Hogg doesn't have a privacy officer. |

| | |
|---|---|
| | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High Almost Certain € 1,000<br>Comments<br>Stefan Sulistyo<br>updated in risk rating<br>3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium Very Likely € 2,500<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High Very Likely € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018<br>- / - 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018<br>- 2 levels / - 20%<br>Mitigation Task Mitigation via Controls<br>Risk Accept Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium Very Likely € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium Almost Certain € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018<br>- 1 level / - 15%<br>Mitigation Task Mitigation via Controls<br>Risk Accept Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High Very Likely € 2,000 |
| **Claim: 11** | |
| 11. A computer-implemented method, the method being performed by a computer system having one or more computer processors and a non-transitory computer readable memory in which programming code is stored, whereupon execution of the programming code by one or more computer processors the computer system performs operations comprising: | |
| | |

| | |
|---|---|
| predicting future cyber threat activity, for each of a plurality of computer network cyber threats, using a Monte Carlo method based on stochastic modeling of actual past observed computer network cyber threat activity, to receive observed cyber threat data from a database, the list of observed cyber threats including information, for each threat, of identification of at least one computer system targeted, to extrapolate future event frequency, to produce a profile of predicted cyber threat activity, wherein for each actual observed cyber threat on the computer network, an identifier, a name, a description of the threat, a temporal profile specifying frequency of occurrence, a target (or targets) for the threat and a severity score for the (each target) are included in the cyber threat data within the database, output the predicted future threat activity to one or more firewalls to improve their accuracy in correctly identifying cyber threats actually observed on the one or more computer networks to improve the accuracy of the apparatus and stochastic modeling of assessing financial loss from cyber threats on an ongoing basis, wherein for each given threat the method comprises; | ALYNE 1;<br><br> alyne<br>Risk Management<br>Tracked Risks<br>Total<br>5<br>Active Risks Tracked<br>4<br>Risks visible in current selection<br>Risk Rating<br>Selection<br>Risks by Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risk Exposure<br>Selection<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Statu<br>new<br>managed<br>Number of selected Risks by current status<br>My Risks<br>All Risks<br>High Risk Cyber Insurance A...<br>Top Risks<br>Vendor Risks<br>New Risk<br>managed<br>High<br>Likely<br>€ 1,000,000<br>Medium<br>Very Likely<br>€ 2,000,000<br>new<br>Medium<br>Likely<br>€ 500,000<br>Medium<br>Unlikely<br>€ 1,500,000<br>Medium: Insufficient BCM<br>High Tech Co has insuffient BCM.<br>Medium: Access Management<br>Applicant Dunder Mifflin has very poor password management.<br>Medium: Cyber Incidents<br>Insufficient transparence of cyber incidents<br>Low: Data Privacy<br>Applicant Wernham Hogg doesn't have a privacy officer. |
| modeling a set of past observed computer network cyber threat events to obtain an estimate of at least one model parameter; | |
| performing a Monte Carlo simulation of the given computer network cyber threat by: | |
| | |
| predicting future computer network cyber threat events using the at least one model parameter and a stochastic model using a projection of at least one | |

| | |
|---|---|
| model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable according to a predefined distribution and to use said at least one variable in the stochastic model and predicting a distribution of future computer network cyber threat events by repeating the simulation using a plurality of variables, determining expected downtime of each IT system in dependence upon said predicted future computer network cyber threat activity, determining financial loss for each of a plurality of operational processes dependent on the downtimes of the IT systems adding losses for the plurality of processes to obtain a combined financial loss arising from the future computer network cyber threat activity. | ALYNE 2;<br><br> Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1<br>5<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - · - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels · - 20%<br>Mitigation Task · Mitigation via Controls · Risk Accept · Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level · - 15%<br>Mitigation Task · Mitigation via Controls · Risk Accept · Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 |
| **Claim: 13** | |
| 13. A computer readable medium having a computer program thereon, which when executed by a computer system having one or more computer processors and a non-transitory computer readable memory, causes the computer system to perform steps comprising: | |
| | |

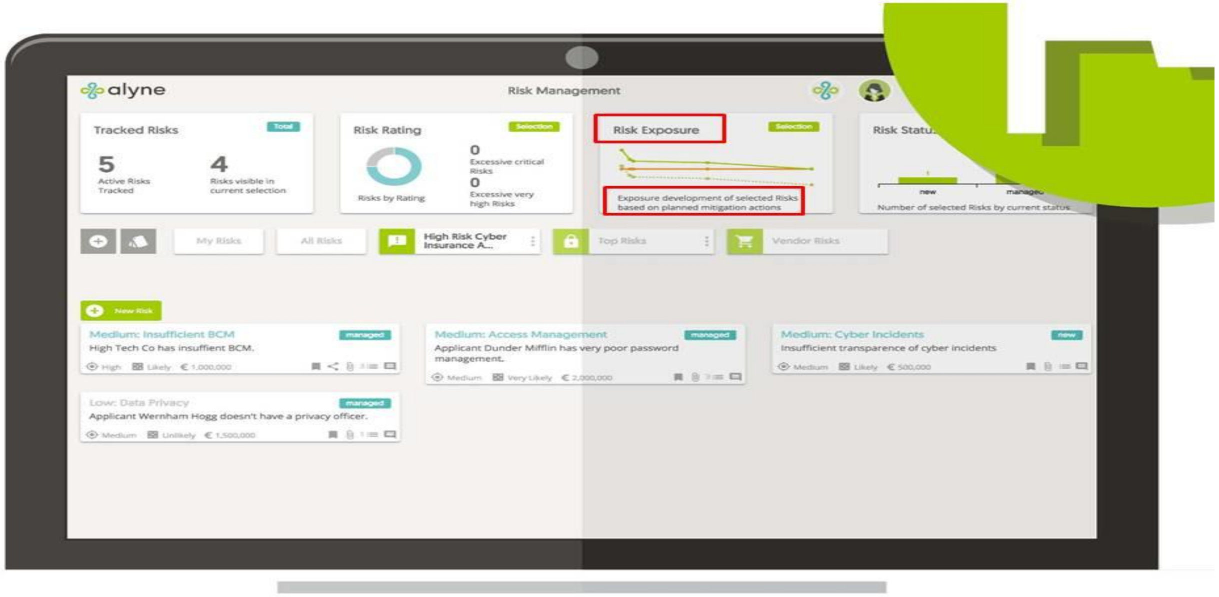
| | |
|---|---|
| to predict, for each of a plurality of computer network cyber threats, future cyber threat activity using a Monte Carlo method based on stochastic modeling of actual past observed computer network cyber threat activity, to receive observed cyber threat data from a database, the list of observed cyber threats including information, for each threat, of identification of at least one computer system targeted, to extrapolate future event frequency, to produce a profile of predicted cyber threat activity, wherein for each actual observed cyber threat on the computer network, an identifier, a name, a description of the threat, a temporal profile specifying frequency of occurrence, a target (or targets) for the threat and a severity score for the (each target) are included in the cyber threat data within the database, output the predicted future threat activity to one or more firewalls to improve their accuracy in correctly identifying cyber threats actually observed on the one or more computer networks to improve the accuracy of the apparatus and stochastic modeling of assessing financial loss from cyber threats on an ongoing basis; | ALYNE 1;<br><br>alyne<br>Risk Management<br>Tracked Risks — Total — 5 Active Risks Tracked — 4 Risks visible in current selection<br>Risk Rating — Selection — Risks by Rating — 0 Excessive critical Risks — 0 Excessive very high Risks<br>Risk Exposure — Selection — Exposure development of selected Risks based on planned mitigation actions<br>Risk Statu — new — manage — Number of selected Risks by current status<br>My Risks — All Risks — High Risk Cyber Insurance A... — Top Risks — Vendor Risks<br>New Risk<br>Medium: Insufficient BCM — managed — High Tech Co has insuffient BCM. — High — Likely — € 1,000,000<br>Medium: Access Management — managed — Applicant Dunder Mifflin has very poor password management. — Medium — Very Likely — € 2,000,000<br>Medium: Cyber Incidents — new — Insufficient transparence of cyber incidents — Medium — Likely — € 500,000<br>Low: Data Privacy — managed — Applicant Wernham Hogg doesn't have a privacy officer. — Medium — Unlikely — € 1,500,000 |
| wherein execution of the computer program causes the computer system to perform, for each given threat, steps further comprising: | |
| modeling a set of past observed computer network cyber threat events to obtain an estimate of at least one model parameter; | |
| performing a Monte Carlo simulation of the given computer network cyber threat by: | |
| predicting future computer network cyber threat events using the at least one model parameter and a | |

| | |
|---|---|
| stochastic model using a projection of at least one model parameter which is based on the estimate of at least one model parameter and on a randomly-drawn variable according to a predefined distribution and to use said at least one variable in the stochastic model and predicting a distribution of future computer network cyber threat events by repeating the simulation using a plurality of variables. | |

**Note:** Total claims: 15 and Independent claims: 3

| **EXHIBIT F** | |
|---|---|
| **Quantar's Preliminary Infringement Contentions** | |
| **US Patent No: 10122751 15/696,202** | **Accused Instrumentalities** |
| **Claim: 1** | |
| 1. A system comprising: | |
| one or more computers comprising one or more hardware processors; | |
| one or more computer-readable media storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising: | |

| | |
|---|---|
| receiving, by the one or more computers, data indicating a list of observed computer-based threats including at least one selected from the group consisting of a virus, malware, a network intrusion, and a denial of service attack, with data for each threat identifying frequency of occurrence, which may include at least one period of time and corresponding frequency of occurrence for a given time window having a beginning and end; | |
| accessing, by the one or more computers, data specifying relationships between: | |
| (i) IT system infrastructures representing computing devices of an organization and a network connecting the computing devices and their physical and logical location, defined by information such as identity, name and category identity; | |
| (ii) system categories indicating characteristics of assets of the organization; | |
| (iii) operational processes of an organization, defined by identity, a name and a value in terms of a monetary value for a given time window having a beginning and end; | |
| | |
| (iv) mitigating actions representing the threat mitigation measures of the organization; | ALYNE 1; |



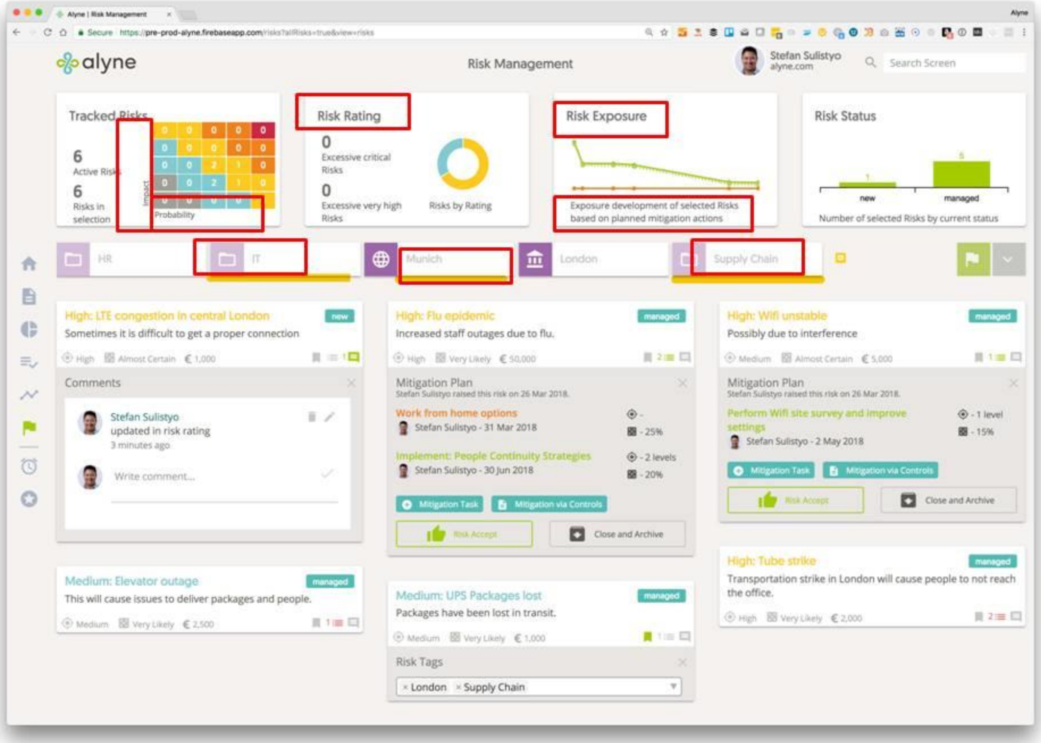
Medium: Insufficient BCM — managed
High Tech Co has insuffient BCM.
High · Likely · € 1,000,000

Medium: Access Management — managed
Applicant Dunder Mifflin has very poor password management.
Medium · Very Likely · € 2,000,000

Medium: Cyber Incidents — new
Insufficient transparence of cyber incidents
Medium · Likely · € 500,000

Low: Data Privacy — managed
Applicant Wernham Hogg doesn't have a privacy officer.
Medium · Unlikely · € 1,500,000

ALYNE 2;



6
Active Risks

6
Risks in selection

| | | | | |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 2 | 1 | 0 |
| 0 | 0 | 2 | 1 | 0 |
| 0 | 0 | 0 | 0 | |

0
Excessive critical Risks

0
Excessive very high Risks

Exposure development of selected Risks based on planned mitigation actions

Number of selected Risks by current status

High: LTE congestion in central London
Sometimes it is difficult to get a proper connection
High · Almost Certain · € 1,000 · 1

Stefan Sulistyo
updated in risk rating
3 minutes ago

Write comment...

Medium: Elevator outage
This will cause issues to deliver packages and people.
Medium · Very Likely · € 2,500 · 1

High: Flu epidemic
Increased staff outages due to flu.
High · Very Likely · € 50,000 · 2

Mitigation Plan
Stefan Sulistyo raised this risk on 26 Mar 2018.

Work from home options
Stefan Sulistyo - 31 Mar 2018 · - · - 25%

Implement: People Continuity Strategies
Stefan Sulistyo - 30 Jun 2018 · - 2 levels · - 20%

Medium: UPS Packages lost
Packages have been lost in transit.
Medium · Very Likely · € 1,000 · 1

× London × Supply Chain

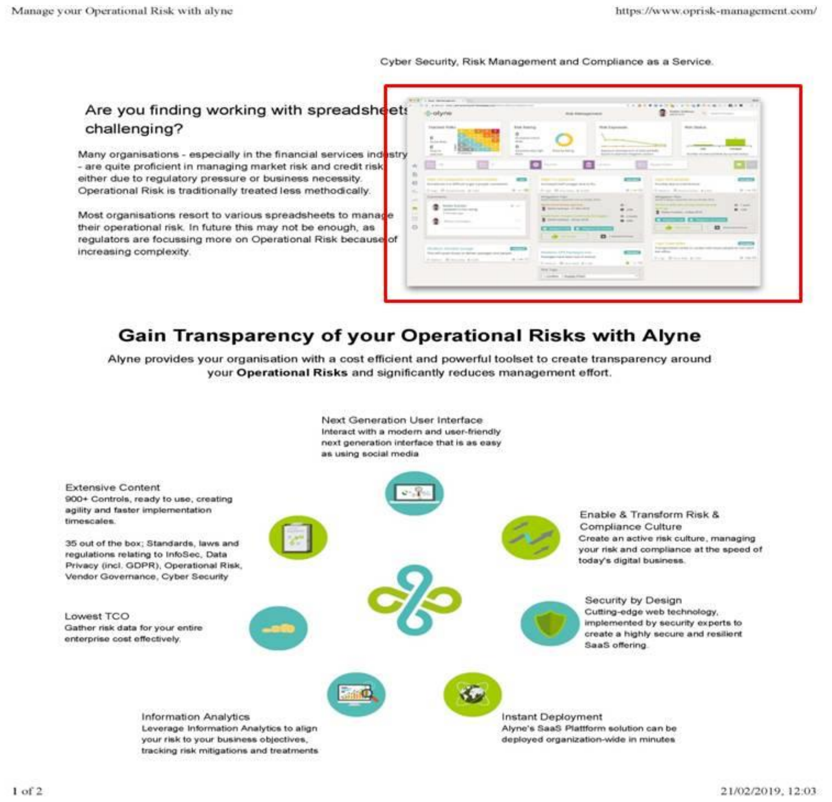
High: Wifi unstable
Possibly due to interference
Medium · Almost Certain · € 5,000 · 1

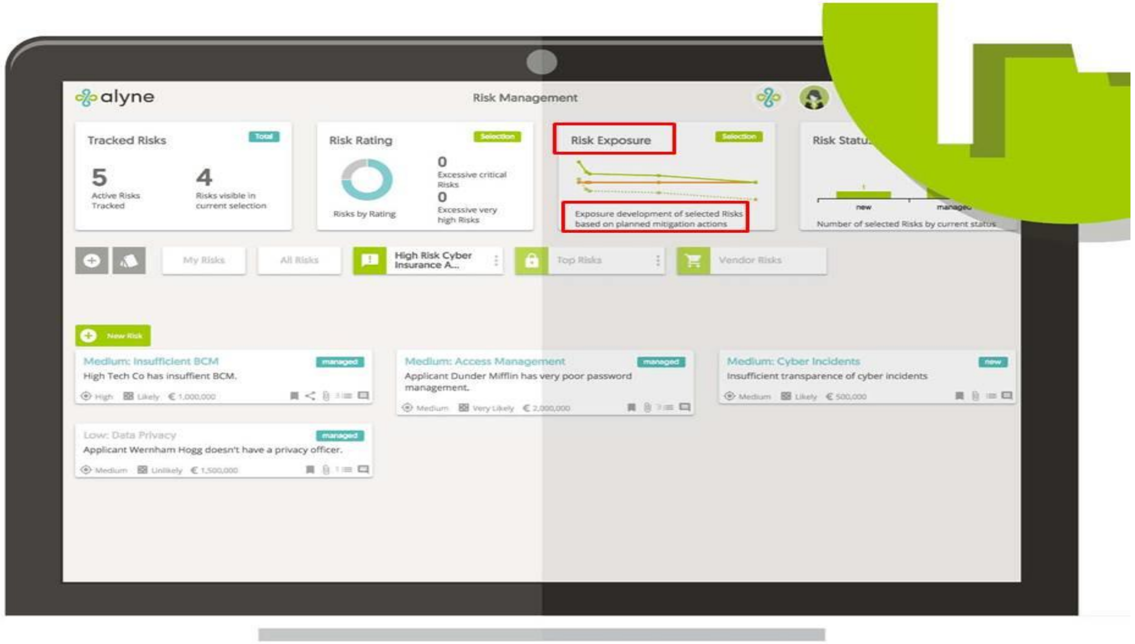
Mitigation Plan
Stefan Sulistyo raised this risk on 26 Mar 2018.

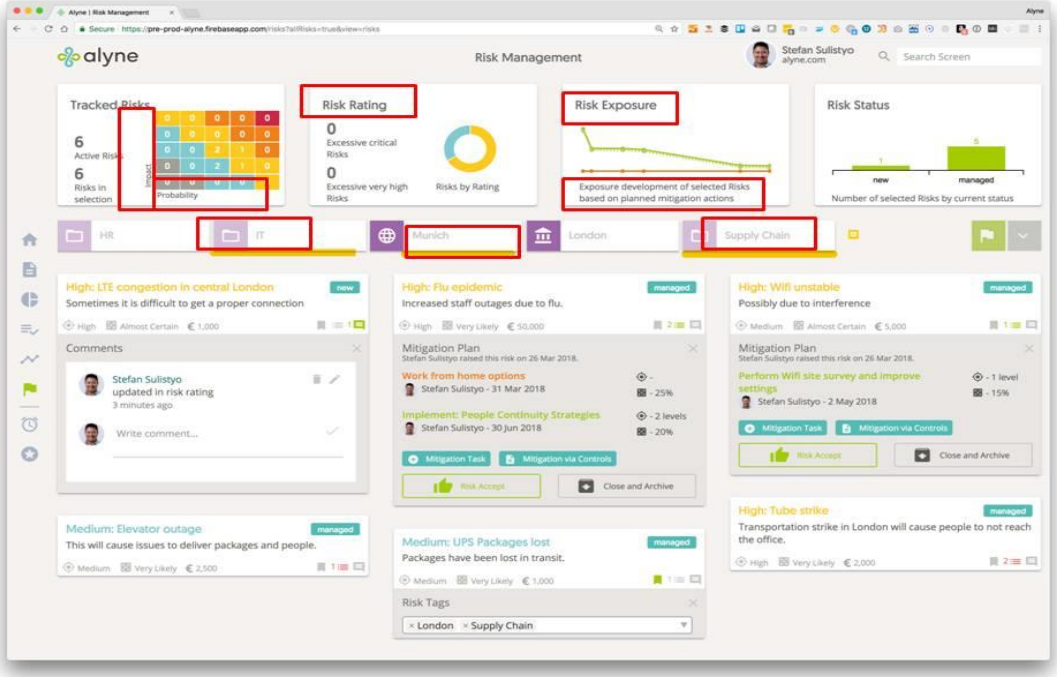
Perform Wifi site survey and improve settings
Stefan Sulistyo - 2 May 2018 · - 1 level · - 15%

High: Tube strike
Transportation strike in London will cause people to not reach the office.
High · Very Likely · € 2,000 · 2

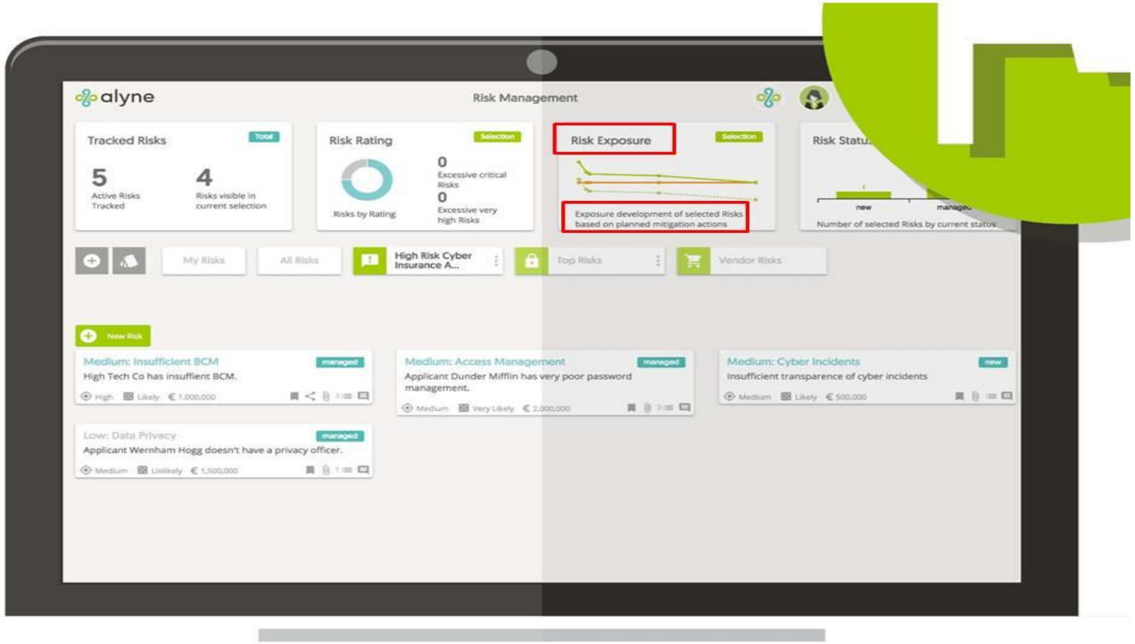
ALYNE 3

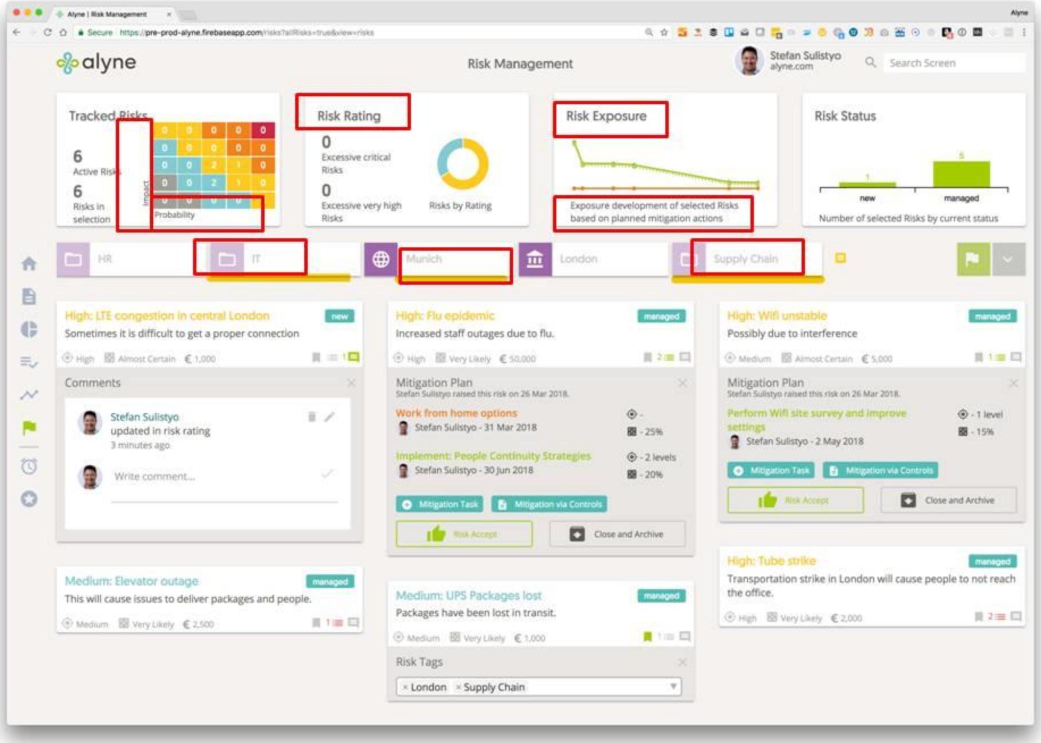
| | |
|---|---|
| | <br>Manage your Operational Risk with alyne https://www.oprisk-management.com/<br>Cyber Security, Risk Management and Compliance as a Service.<br>Are you finding working with spreadsheets challenging?<br>Many organisations - especially in the financial services industry - are quite proficient in managing market risk and credit risk either due to regulatory pressure or business necessity. Operational Risk is traditionally treated less methodically.<br>Most organisations resort to various spreadsheets to manage their operational risk. In future this may not be enough, as regulators are focussing more on Operational Risk because of increasing complexity.<br>**Gain Transparency of your Operational Risks with Alyne**<br>Alyne provides your organisation with a cost efficient and powerful toolset to create transparency around your **Operational Risks** and significantly reduces management effort.<br>Next Generation User Interface<br>Interact with a modern and user-friendly next generation interface that is as easy as using social media<br>Extensive Content<br>900+ Controls, ready to use, creating agility and faster implementation timescales.<br>35 out of the box; Standards, laws and regulations relating to InfoSec, Data Privacy (incl. GDPR), Operational Risk, Vendor Governance, Cyber Security<br>Enable & Transform Risk & Compliance Culture<br>Create an active risk culture, managing your risk and compliance at the speed of today's digital business.<br>Lowest TCO<br>Gather risk data for your entire enterprise cost effectively.<br>Security by Design<br>Cutting-edge web technology, implemented by security experts to create a highly secure and resilient SaaS offering.<br>Information Analytics<br>Leverage Information Analytics to align your risk to your business objectives, tracking risk mitigations and treatments<br>Instant Deployment<br>Alyne's SaaS Plattform solution can be deployed organization-wide in minutes<br>1 of 2 21/02/2019, 12:03 |
| performing, by the one or more computers a plurality of simulations using a Monte Carlo method using the accessed data specifying relationships to predict a distribution of threat events, each simulation involving propagating data through stochastic modelling for a given time window having a beginning and end; | |
| | |

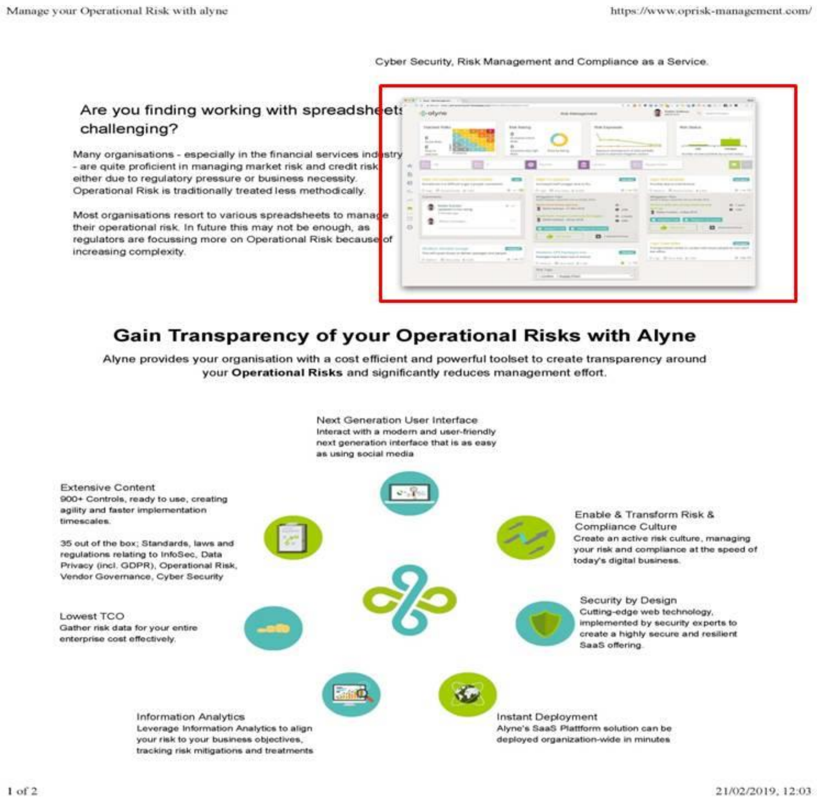
| | |
|---|---|
| modelling threat events using at least two different stochastic models and obtaining at least two different sets of model parameters, sampling, by the one or more computers, outcomes of the plurality of simulations generated using a Monte Carlo method according to the set of threat events within a series of temporal profiles, each having a beginning and end; | ALYNE 1;<br><br> alyne<br>Risk Management<br>Tracked Risks<br>Total<br>5<br>Active Risks Tracked<br>4<br>Risks visible in current selection<br>Risk Rating<br>Selection<br>Risks by Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risk Exposure<br>Selection<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Statu<br>new<br>managed<br>Number of selected Risks by current status<br>My Risks<br>All Risks<br>High Risk Cyber Insurance A...<br>Top Risks<br>Vendor Risks<br>New Risk<br>Medium: Insufficient BCM<br>managed<br>High Tech Co has insuffient BCM.<br>High<br>Likely<br>€ 1,000,000<br>Medium: Access Management<br>managed<br>Applicant Dunder Mifflin has very poor password management.<br>Medium<br>Very Likely<br>€ 2,000,000<br>Medium: Cyber Incidents<br>new<br>Insufficient transparence of cyber incidents<br>Medium<br>Likely<br>€ 500,000<br>Low: Data Privacy<br>managed<br>Applicant Wernham Hogg doesn't have a privacy officer.<br>Medium<br>Unlikely<br>€ 1,500,000 |
| sampling, by the one or more computers, a plurality of simulation outcomes of the plurality of simulations generated using a Monte Carlo method that include mitigating actions representing the threat mitigation measures of the organization for a series of given time windows, each having a beginning and end; | |
| | |
| based on the sampled outcomes of the simulations, determining, by the one or more computers, measures of impact of the computer-related threats to the organization for a given time window having a beginning and end and | ALYNE 2; |

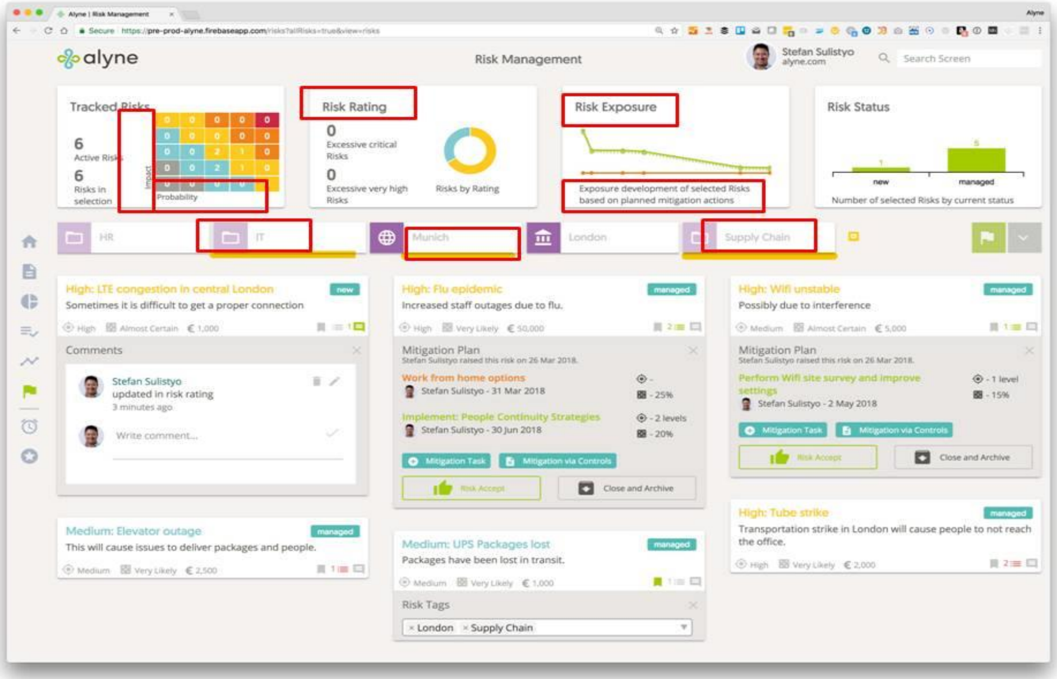
| | |
|---|---|
| providing, by the one or more computers and for output to a user, graphical representations of the determined measures of impact of the computer-based threats to the organization, for a given time window having a beginning and end, in a graphical user interface; | <br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>0 0 0 0 0<br>0 0 0 0 0<br>0 0 2 1 0<br>0 0 2 1 0<br>0 0 0 0<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1 new<br>5 managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000 · 1<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500 · 1<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000 · 2<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - · - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels · - 20%<br>Mitigation Task · Mitigation via Controls<br>Risk Accept · Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000 · 1<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000 · 1<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level · - 15%<br>Mitigation Task · Mitigation via Controls<br>Risk Accept · Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 · 2 |
| the one or more computers further configured to; | |
| receive observed computer-based threat data; | |
| receive input data of the number of viruses contracted by period and the number of new viruses worldwide; | |
| extrapolating from the input data, using a Monte Carlo method, to predict future computer-based threat activity rates and types and; | |
| outputting said predicted future computer-based threat activity into the network and firewall logs, updating the firewall policy tree to define the | |

| | |
|---|---|
| action of accept or deny, according to the changes automatically made to the policy tree of rules in the sets of firewall rules, which in turn inserts updated rules into the firewall policy. | |
| **Claim: 9** | |
| 9. A method performed by one or more computers, the method comprising: | |
| receiving and accessing, by the one or more computers, data specifying relationships between: | |
| (i) IT system infrastructures representing computing devices of an organization and a network connecting the computing devices and their physical and logical location, defined by information such as identity, name and category identity; | |
| (ii) system categories indicating characteristics of assets of the organization; | |
| (iii) operational processes of an organization, defined by identity, a name and a value in terms of a monetary value for a given time window having a beginning and end; | |
| (iii) a list of observed computer-based threats including at least one selected from the group consisting of a virus, malware, a network intrusion, and a denial of service attack, with data for each threat identifying frequency of occurrence, which may include at least one period of time and corresponding frequency of occurrence for a given time window having a beginning and end; | |

| | |
|---|---|
| (iv) mitigating actions representing the threat mitigation measures of the organization; | ALYNE 1;<br><br>alyne<br>Risk Management<br>Tracked Risks Total<br>5 Active Risks Tracked<br>4 Risks visible in current selection<br>Risk Rating Selection<br>Risks by Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risk Exposure Selection<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Statu<br>new managed<br>Number of selected Risks by current status<br>My Risks<br>All Risks<br>High Risk Cyber Insurance A...<br>Top Risks<br>Vendor Risks<br>New Risk<br>Medium: Insufficient BCM managed<br>High Tech Co has insuffient BCM.<br>High Likely € 1,000,000<br>Medium: Access Management managed<br>Applicant Dunder Mifflin has very poor password management.<br>Medium Very Likely € 2,000,000<br>Medium: Cyber Incidents new<br>Insufficient transparence of cyber incidents<br>Medium Likely € 500,000<br>Low: Data Privacy managed<br>Applicant Wernham Hogg doesn't have a privacy officer.<br>Medium Unlikely € 1,500,000<br>ALYNE 2; |

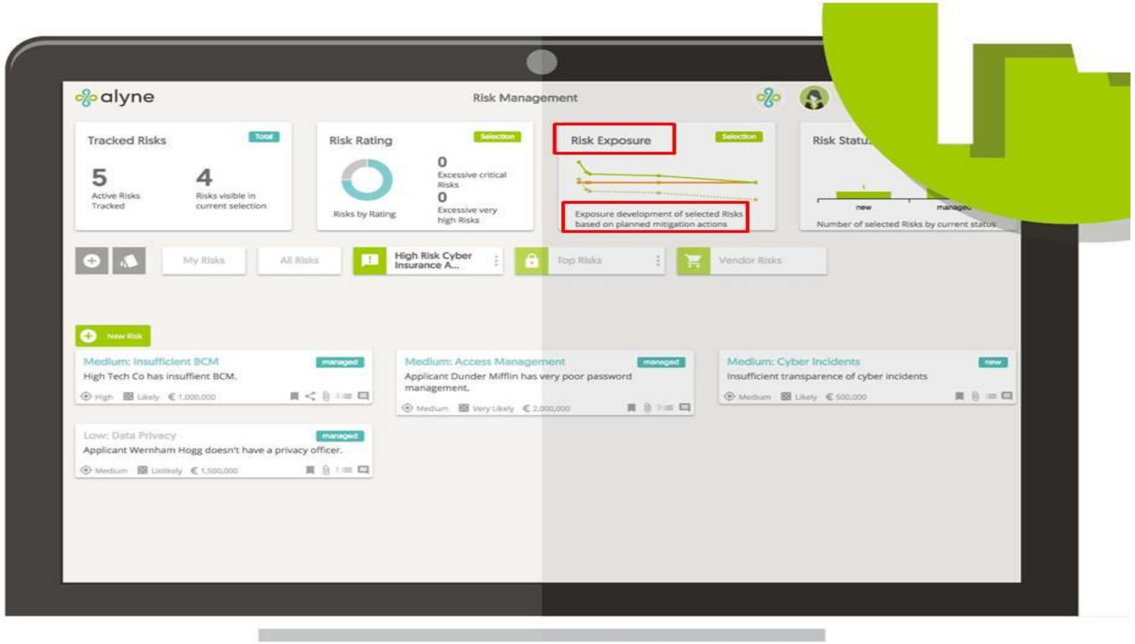
| | |
|---|---|
| | <br>Alyne \| Risk Management<br>https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo<br>updated in risk rating<br>3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - · - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels · - 20%<br>Mitigation Task · Mitigation via Controls<br>Risk Accept · Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level · - 15%<br>Mitigation Task · Mitigation via Controls<br>Risk Accept · Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000<br><br>ALYNE 3 |

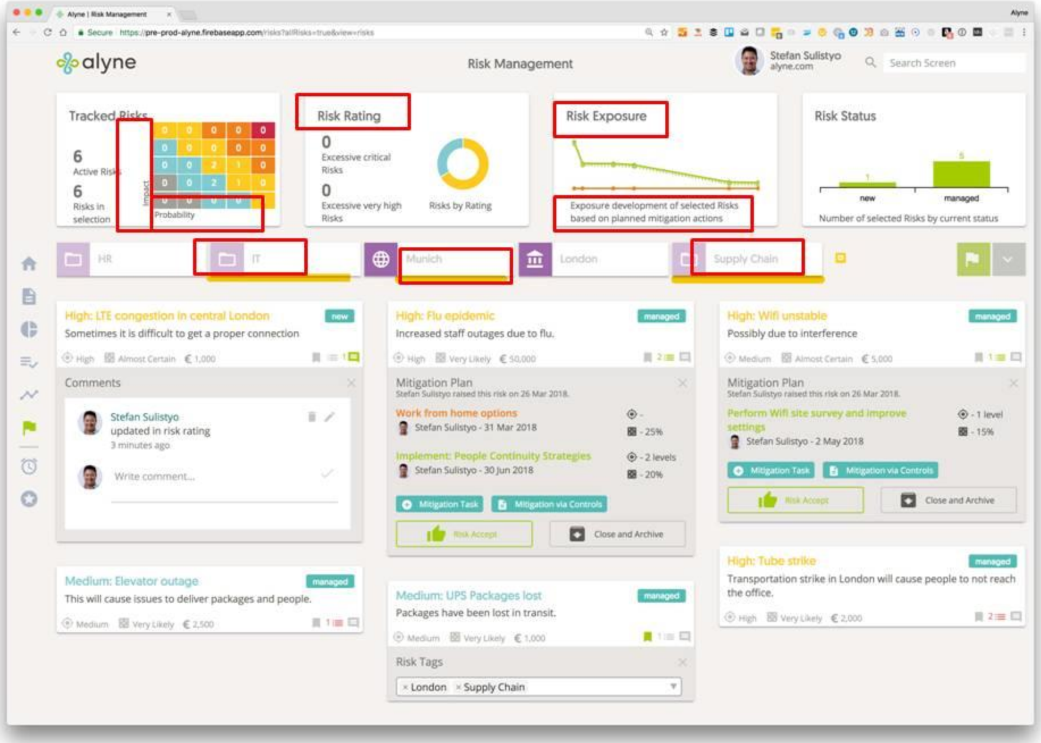
| | |
|---|---|
| | <br>Manage your Operational Risk with alyne https://www.oprisk-management.com/<br>Cyber Security, Risk Management and Compliance as a Service.<br>**Are you finding working with spreadsheets challenging?**<br>Many organisations - especially in the financial services industry - are quite proficient in managing market risk and credit risk either due to regulatory pressure or business necessity. Operational Risk is traditionally treated less methodically.<br>Most organisations resort to various spreadsheets to manage their operational risk. In future this may not be enough, as regulators are focussing more on Operational Risk because of increasing complexity.<br>**Gain Transparency of your Operational Risks with Alyne**<br>Alyne provides your organisation with a cost efficient and powerful toolset to create transparency around your **Operational Risks** and significantly reduces management effort.<br>Next Generation User Interface<br>Interact with a modern and user-friendly next generation interface that is as easy as using social media<br>Extensive Content<br>900+ Controls, ready to use, creating agility and faster implementation timescales.<br>35 out of the box; Standards, laws and regulations relating to InfoSec, Data Privacy (incl. GDPR), Operational Risk, Vendor Governance, Cyber Security<br>Enable & Transform Risk & Compliance Culture<br>Create an active risk culture, managing your risk and compliance at the speed of today's digital business.<br>Lowest TCO<br>Gather risk data for your entire enterprise cost effectively.<br>Security by Design<br>Cutting-edge web technology, implemented by security experts to create a highly secure and resilient SaaS offering.<br>Information Analytics<br>Leverage Information Analytics to align your risk to your business objectives, tracking risk mitigations and treatments<br>Instant Deployment<br>Alyne's SaaS Plattform solution can be deployed organization-wide in minutes<br>1 of 2 21/02/2019, 12:03 |
| the one or more computers performing a plurality of simulations using a Monte Carlo method using the accessed data specifying relationships, each simulation involving propagating data through stochastic modeling for a given time window having a beginning and end; | |
| sampling by the one or more computers, outcomes of the plurality of simulations generated using a Monte Carlo method, for a given time window having a beginning and end; | |

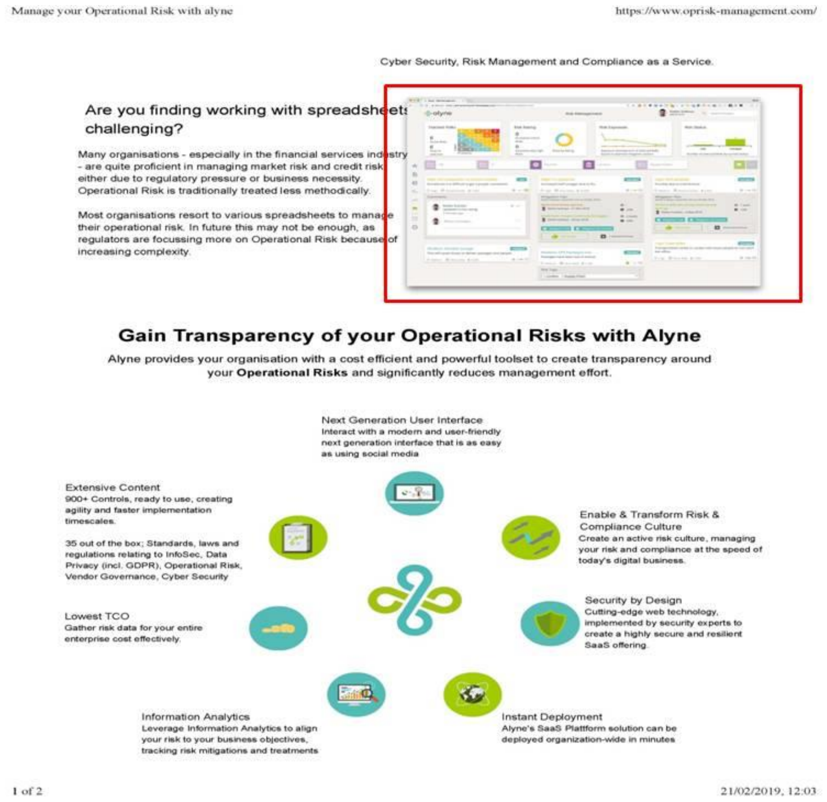
| | |
|---|---|
| sampling by the one or more computers, outcomes of the plurality of simulations generated using a Monte Carlo method, that include mitigating actions representing the threat mitigation measures of the organization for a given time window having a beginning and end; | |
| | |
| performing, based on the sampled outcomes of the simulations generated using a Monte Carlo method, determining, by the one or more computers, measures of impact of the computer-related threats to the organization for a given time window having a beginning and end and providing, by the one or more computers and for output to a user, graphical representations of the determined measures of impact of the computer-based threats to the organization, for a given time window having a beginning and end, in a graphical user interface; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>0 0 0 0 0<br>0 0 0 0 0<br>0 0 2 1 0<br>0 0 2 1 0<br>0 0 0 0<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1 5<br>new managed<br>Number of selected Risks by current status<br>HR IT Munich London Supply Chain<br>High: LTE congestion in central London new<br>Sometimes it is difficult to get a proper connection<br>High Almost Certain € 1,000 1<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage managed<br>This will cause issues to deliver packages and people.<br>Medium Very Likely € 2,500 1<br>High: Flu epidemic managed<br>Increased staff outages due to flu.<br>High Very Likely € 50,000 2<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options - - 25%<br>Stefan Sulistyo - 31 Mar 2018<br>Implement: People Continuity Strategies - 2 levels - 20%<br>Stefan Sulistyo - 30 Jun 2018<br>Mitigation Task Mitigation via Controls<br>Risk Accept Close and Archive<br>Medium: UPS Packages lost managed<br>Packages have been lost in transit.<br>Medium Very Likely € 1,000 1<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable managed<br>Possibly due to interference<br>Medium Almost Certain € 5,000 1<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings - 1 level - 15%<br>Stefan Sulistyo - 2 May 2018<br>Mitigation Task Mitigation via Controls<br>Risk Accept Close and Archive<br>High: Tube strike managed<br>Transportation strike in London will cause people to not reach the office.<br>High Very Likely € 2,000 2 |
| receive observed computer-based threat data; | |

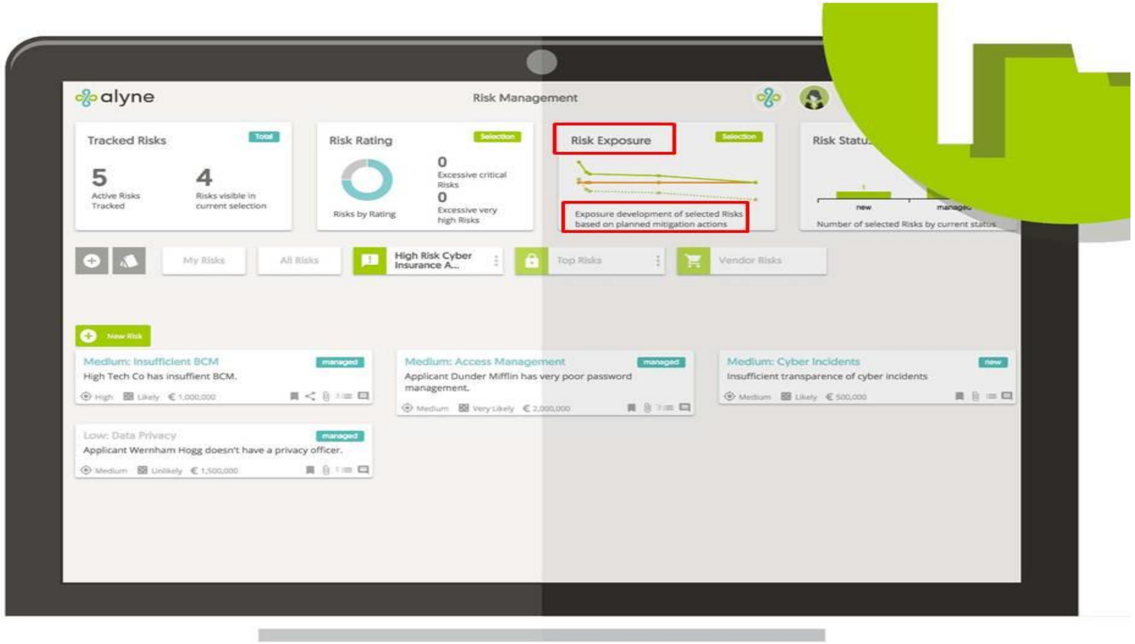
| | |
|---|---|
| receive input data of the number of viruses contracted by period and the number of new viruses worldwide; | |
| extrapolating from the input data, using a Monte Carlo method, to predict future computer-based threat activity rates and types and; | |
| outputting said predicted future computer-based threat activity to one or more firewalls, to improve accuracy in identifying computer based threats on the one or more computer networks, strengthen their accuracy through the detection of anomalous firewall policy rules, into the network and firewall logs, updating the firewall policy tree to define the action of accept or deny, according to the changes automatically made to the policy tree of rules in the sets of firewall rules, which in turn inserts updated rules into the firewall policy, wherein the method is performed by one or more computers comprising one or more hardware processors; | |
| one or more computer-readable media storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising. | |
| **Claim: 17** | |
| 17. A non-transitory computer-readable medium storing instructions that, when executed by the one or more computers, cause the one or more computers to perform operations comprising: | |
| receiving and accessing, by the one or more computers, data specifying relationships between: | |

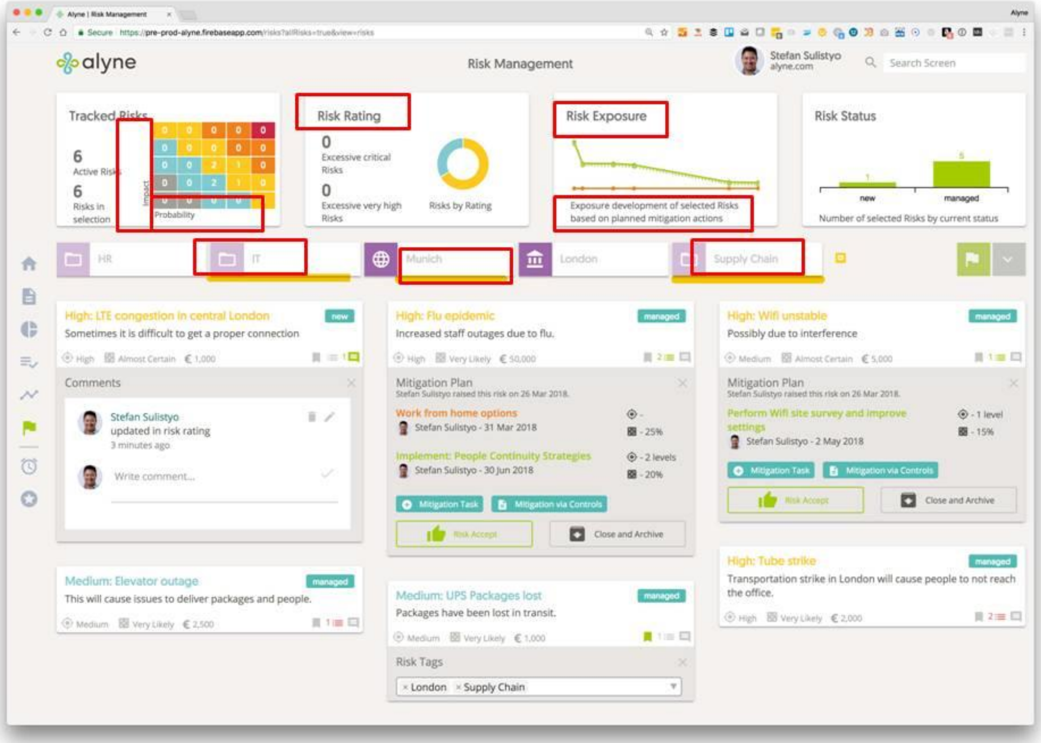
| | |
|---|---|
| (i) IT system infrastructures representing computing devices of an organization and a network connecting the computing devices and their physical and logical location, defined by information such as identity, name and category identity; | |
| (ii) system categories indicating characteristics of assets of the organization; | |
| (iii) operational processes of an organization, defined by identity, a name and a value in terms of a monetary value for a given time window having a beginning and end; | |
| (iv) a list of observed computer-based threats including at least one selected from the group consisting of a virus, malware, a network intrusion, and a denial of service attack, with data for each threat identifying frequency of occurrence, which may include at least one period of time and corresponding frequency of occurrence for a given time window having a beginning and end; | |
| | |
| (iv) mitigating actions representing the threat mitigation measures of the organization; | ALYNE 1; |

| | |
|---|---|
| | <br> alyne<br>Risk Management<br>Tracked Risks<br>Total<br>5<br>Active Risks Tracked<br>4<br>Risks visible in current selection<br>Risk Rating<br>Selection<br>Risks by Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risk Exposure<br>Selection<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Statu<br>new<br>managed<br>Number of selected Risks by current status<br>My Risks<br>All Risks<br>High Risk Cyber Insurance A...<br>Top Risks<br>Vendor Risks<br>New Risk<br>Medium: Insufficient BCM<br>managed<br>High Tech Co has insuffient BCM.<br>High Likely € 1,000,000<br>Medium: Access Management<br>managed<br>Applicant Dunder Mifflin has very poor password management.<br>Medium Very Likely € 2,000,000<br>Medium: Cyber Incidents<br>new<br>Insufficient transparence of cyber incidents<br>Medium Likely € 500,000<br>Low: Data Privacy<br>managed<br>Applicant Wernham Hogg doesn't have a privacy officer.<br>Medium Unlikely € 1,500,000<br><br>ALYNE 2; |

| | |
|---|---|
| | <br> Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>Alyne<br>alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>Impact<br>Probability<br>Risk Rating<br>Risks by Rating<br>Risk Exposure<br>Risk Status<br>1<br>5<br>new<br>managed<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>6 Active Risks<br>6 Risks in selection<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Exposure development of selected Risks based on planned mitigation actions<br>Number of selected Risks by current status<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000 · 1<br>Comments<br>Stefan Sulistyo updated in risk rating<br>3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500 · 1<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000 · 2<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 · - · - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 · - 2 levels · - 20%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000 · 1<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000 · 1<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 · - 1 level · - 15%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 · 2<br><br>ALYNE 3 |

| | |
|---|---|
| | <br>Manage your Operational Risk with alyne https://www.oprisk-management.com/<br>Cyber Security, Risk Management and Compliance as a Service.<br>Are you finding working with spreadsheets challenging?<br>Many organisations - especially in the financial services industry - are quite proficient in managing market risk and credit risk either due to regulatory pressure or business necessity. Operational Risk is traditionally treated less methodically.<br>Most organisations resort to various spreadsheets to manage their operational risk. In future this may not be enough, as regulators are focussing more on Operational Risk because of increasing complexity.<br>Gain Transparency of your Operational Risks with Alyne<br>Alyne provides your organisation with a cost efficient and powerful toolset to create transparency around your **Operational Risks** and significantly reduces management effort.<br>Next Generation User Interface<br>Interact with a modern and user-friendly next generation interface that is as easy as using social media<br>Extensive Content<br>900+ Controls, ready to use, creating agility and faster implementation timescales.<br>35 out of the box; Standards, laws and regulations relating to InfoSec, Data Privacy (incl. GDPR), Operational Risk, Vendor Governance, Cyber Security<br>Enable & Transform Risk & Compliance Culture<br>Create an active risk culture, managing your risk and compliance at the speed of today's digital business.<br>Security by Design<br>Cutting-edge web technology, implemented by security experts to create a highly secure and resilient SaaS offering.<br>Lowest TCO<br>Gather risk data for your entire enterprise cost effectively.<br>Information Analytics<br>Leverage Information Analytics to align your risk to your business objectives, tracking risk mitigations and treatments<br>Instant Deployment<br>Alyne's SaaS Plattform solution can be deployed organization-wide in minutes<br>1 of 2 21/02/2019, 12:03 |
| the one or more computers performing a plurality of simulations using a Monte Carlo method, each simulation involving propagating data through stochastic modeling for a given time window having a beginning and end; | |
| sampling by the one or more computers using the accessed data specifying relationships, outcomes of the plurality of simulations for a given time window having a beginning and end; | |
| | |

| | |
|---|---|
| sampling by the one or more computers using the accessed data specifying relationships, outcomes of the plurality of simulations that include mitigating actions representing the threat mitigation measures of the organization for a given time window having a beginning and end; | ALYNE 1;<br><br> alyne<br>Risk Management<br>Tracked Risks<br>Total<br>5<br>Active Risks Tracked<br>4<br>Risks visible in current selection<br>Risk Rating<br>Selection<br>Risks by Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risk Exposure<br>Selection<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Statu<br>new<br>managed<br>Number of selected Risks by current status<br>My Risks<br>All Risks<br>High Risk Cyber Insurance A...<br>Top Risks<br>Vendor Risks<br>New Risk<br>Medium: Insufficient BCM<br>managed<br>High<br>Likely<br>€ 1,000,000<br>Medium: Access Management<br>managed<br>Medium<br>Very Likely<br>€ 2,000,000<br>Medium: Cyber Incidents<br>new<br>Medium<br>Likely<br>€ 500,000<br>Low: Data Privacy<br>managed<br>Medium<br>Unlikely<br>€ 1,500,000<br>High Tech Co has insuffient BCM.<br>Applicant Dunder Mifflin has very poor password management.<br>Insufficient transparence of cyber incidents<br>Applicant Wernham Hogg doesn't have a privacy officer.<br>ALYNE 2; |



High: LTE congestion in central London — new

Sometimes it is difficult to get a proper connection

High · Almost Certain · € 1,000

Comments

Stefan Sulistyo updated in risk rating
3 minutes ago

Write comment...

Medium: Elevator outage — managed

This will cause issues to deliver packages and people.

Medium · Very Likely · € 2,500

High: Flu epidemic — managed

Increased staff outages due to flu.

High · Very Likely · € 50,000

Mitigation Plan
Stefan Sulistyo raised this risk on 26 Mar 2018.

Work from home options — Stefan Sulistyo - 31 Mar 2018 — - ; - 25%

Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels; - 20%

Mitigation Task · Mitigation via Controls · Risk Accept · Close and Archive

Medium: UPS Packages lost — managed

Packages have been lost in transit.

Medium · Very Likely · € 1,000

Risk Tags: × London × Supply Chain

High: Wifi unstable — managed

Possibly due to interference

Medium · Almost Certain · € 5,000

Mitigation Plan
Stefan Sulistyo raised this risk on 26 Mar 2018.

Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level; - 15%

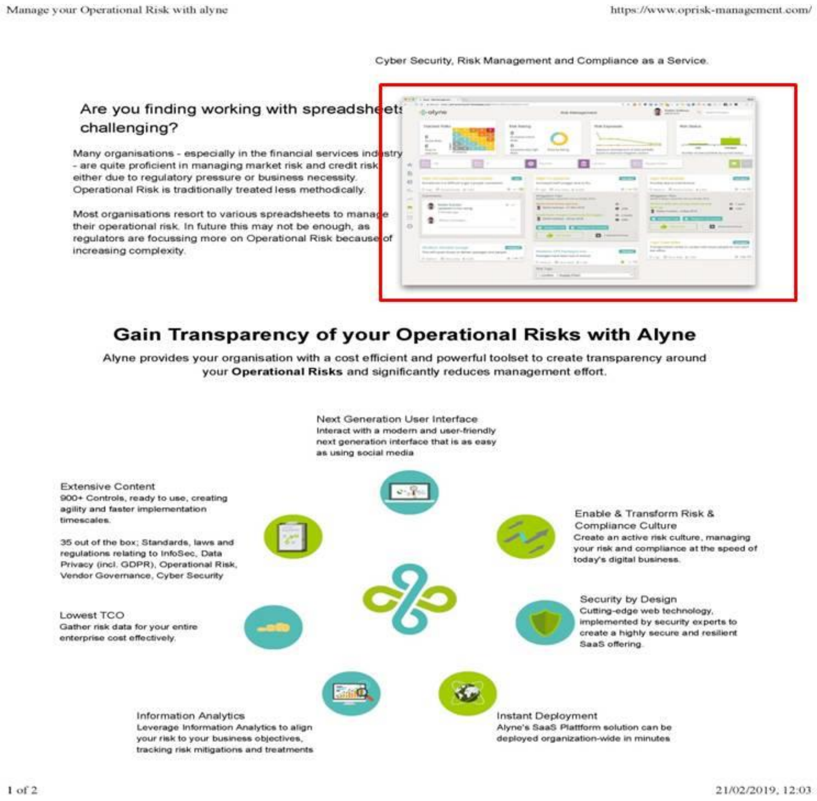
Mitigation Task · Mitigation via Controls · Risk Accept · Close and Archive

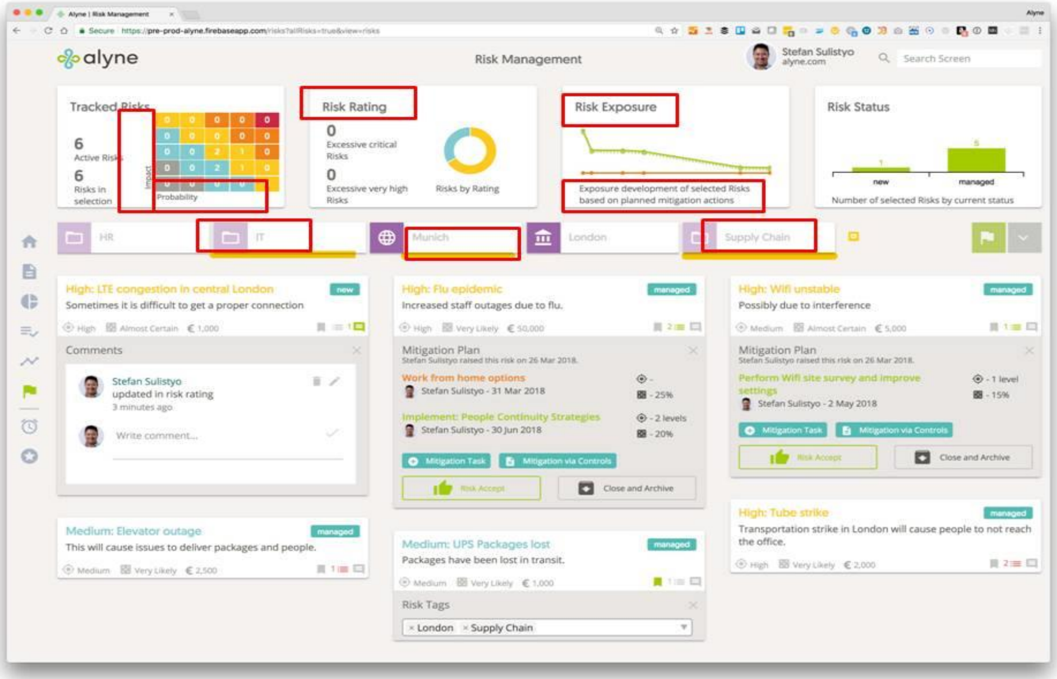
High: Tube strike — managed

Transportation strike in London will cause people to not reach the office.

High · Very Likely · € 2,000

ALYNE 3

| | |
|---|---|
| | <br>Manage your Operational Risk with alyne https://www.oprisk-management.com/<br>Cyber Security, Risk Management and Compliance as a Service.<br>**Are you finding working with spreadsheets challenging?**<br>Many organisations - especially in the financial services industry - are quite proficient in managing market risk and credit risk either due to regulatory pressure or business necessity. Operational Risk is traditionally treated less methodically.<br>Most organisations resort to various spreadsheets to manage their operational risk. In future this may not be enough, as regulators are focussing more on Operational Risk because of increasing complexity.<br>**Gain Transparency of your Operational Risks with Alyne**<br>Alyne provides your organisation with a cost efficient and powerful toolset to create transparency around your **Operational Risks** and significantly reduces management effort.<br>Next Generation User Interface<br>Interact with a modern and user-friendly next generation interface that is as easy as using social media<br>Extensive Content<br>900+ Controls, ready to use, creating agility and faster implementation timescales.<br>35 out of the box; Standards, laws and regulations relating to InfoSec, Data Privacy (incl. GDPR), Operational Risk, Vendor Governance, Cyber Security<br>Enable & Transform Risk & Compliance Culture<br>Create an active risk culture, managing your risk and compliance at the speed of today's digital business.<br>Lowest TCO<br>Gather risk data for your entire enterprise cost effectively.<br>Security by Design<br>Cutting-edge web technology, implemented by security experts to create a highly secure and resilient SaaS offering.<br>Information Analytics<br>Leverage Information Analytics to align your risk to your business objectives, tracking risk mitigations and treatments<br>Instant Deployment<br>Alyne's SaaS Plattform solution can be deployed organization-wide in minutes<br>1 of 2 21/02/2019, 12:03 |
| | |
| based on the sampled outcomes of the simulations, determining, by the one or more computers, measures of impact of the computer-related threats to the organization for a given time window having a beginning and end and providing, by the one or more computers and for output to a user, graphical representations of the determined measures of impact of the computer-based threats to the organization, for a given time | ALYNE 2; |

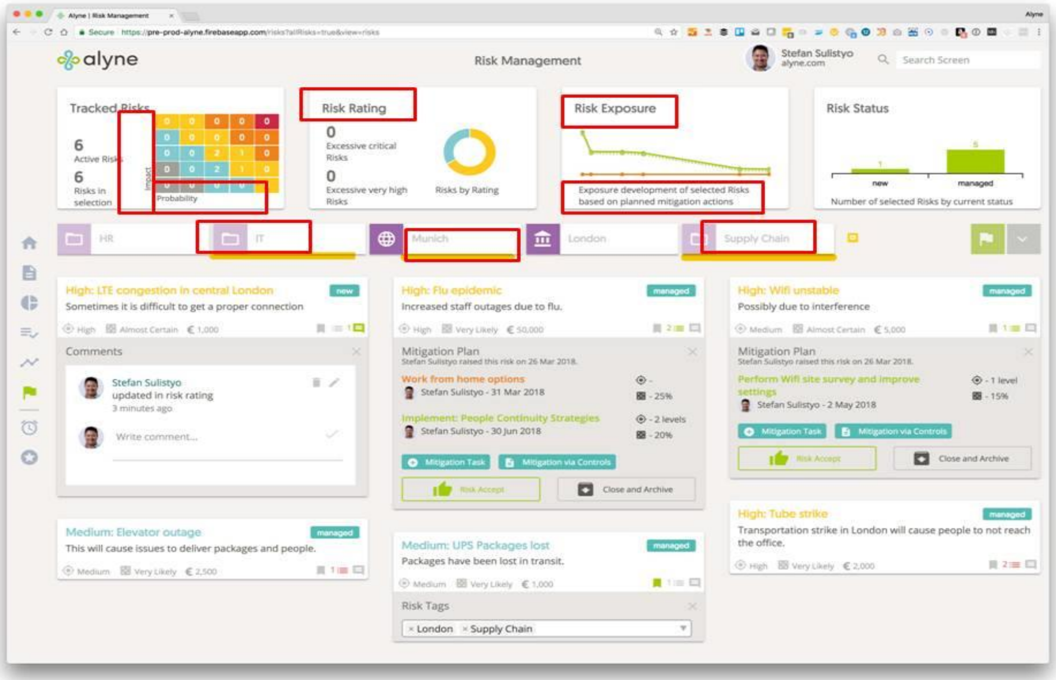
| | |
|---|---|
| window having a beginning and end, in a graphical user interface; | <br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne<br>Risk Management<br>Stefan Sulistyo alyne.com<br>Search Screen<br>Tracked Risks<br>6 Active Risks<br>6 Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0 Excessive critical Risks<br>0 Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London new<br>Sometimes it is difficult to get a proper connection<br>High Almost Certain € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage managed<br>This will cause issues to deliver packages and people.<br>Medium Very Likely € 2,500<br>High: Flu epidemic managed<br>Increased staff outages due to flu.<br>High Very Likely € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options<br>Stefan Sulistyo - 31 Mar 2018<br>- 25%<br>Implement: People Continuity Strategies<br>Stefan Sulistyo - 30 Jun 2018<br>- 2 levels<br>- 20%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost managed<br>Packages have been lost in transit.<br>Medium Very Likely € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable managed<br>Possibly due to interference<br>Medium Almost Certain € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings<br>Stefan Sulistyo - 2 May 2018<br>- 1 level<br>- 15%<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike managed<br>Transportation strike in London will cause people to not reach the office.<br>High Very Likely € 2,000 |
| the one or more computers further configured to; | |
| receive observed computer-based threat data; | |
| receive input data of the number of viruses contracted by period and the number of new viruses worldwide; | |
| extrapolating from the input data, using a Monte Carlo method, to predict future computer-based threat activity rates and types and; | |
| outputting said predicted future computer-based threat activity to one or more firewalls, to improve accuracy in identifying computer based threats on | |

|  |  |
|---|---|
| the one or more computer networks, strengthen their accuracy through the detection of anomalous firewall policy rules, into the network and firewall logs, updating the firewall policy tree to define the action of accept or deny, according to the changes automatically made to the policy tree of rules in the sets of firewall rules, which in turn inserts updated rules into the firewall policy. |  |

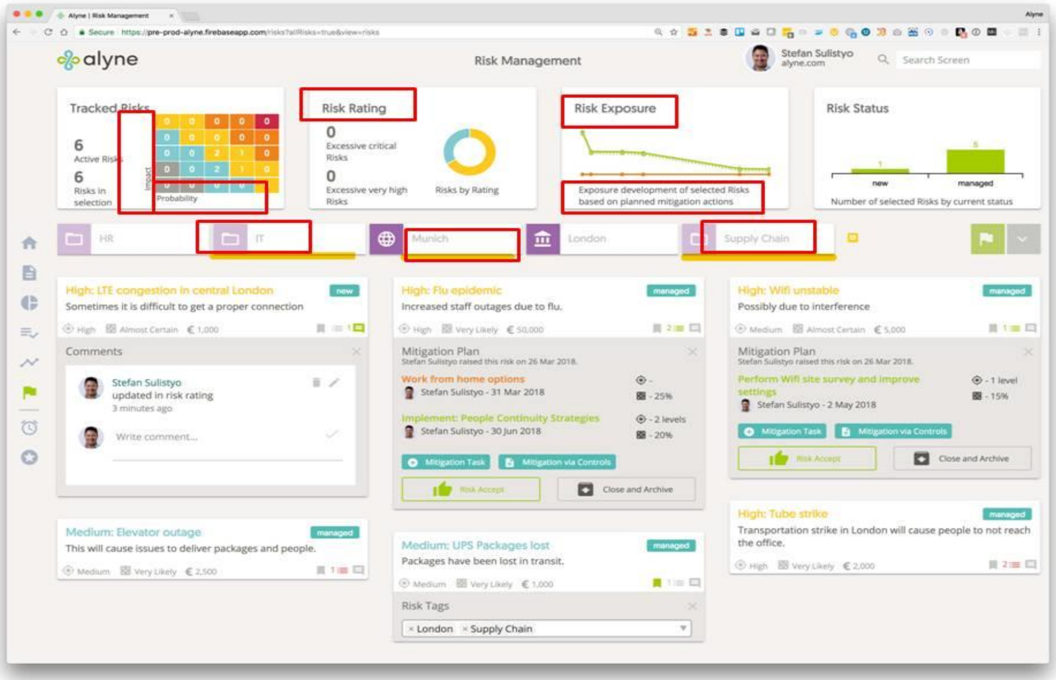
**Note:** Total claims: 20 and Independent claims: 3

| **EXHIBIT G** |  |
|---|---|
| **Quantar's Preliminary Infringement Contentions** |  |
| **US Patent Application No: 20180039922**<br>**15/231,131** | **Accused Instrumentalities** |
| **Claim: 1** |  |
| 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: |  |

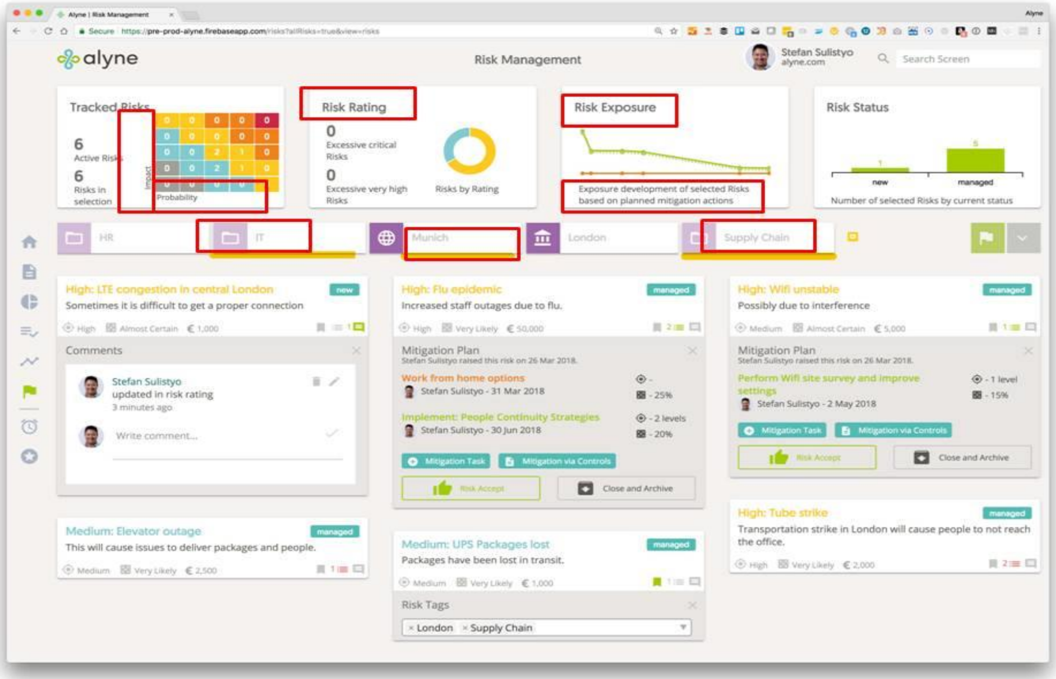
| | |
|---|---|
| predict for each electronic threat capable of affecting computer networks in which IT systems operate, future threat activity based on past electronic threat activity wherein the electronic threats include computer viruses, Trojan horses, computer worms, malware, malicious signed binaries, 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 in dependence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br>Alyne \| Risk Management<br>https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br> alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6<br>Active Risks<br>6<br>Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1<br>5<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - · - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels · - 20%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level · - 15%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 |
| 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. |  |
| **Claim: 13** |  |
| 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 in dependence upon said predicted electronic threat activity including the severity scores and extrapolated future event frequency; | ALYNE 2;<br><br>Alyne \| Risk Management<br>https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br>alyne Risk Management Stefan Sulistyo alyne.com Search Screen<br>Tracked Risks: 6 Active Risks; 6 Risks in selection<br>Risk Rating: 0 Excessive critical Risks; 0 Excessive very high Risks; Risks by Rating<br>Risk Exposure: Exposure development of selected Risks based on planned mitigation actions<br>Risk Status: Number of selected Risks by current status<br>HR · IT · Munich · London · Supply Chain<br>High: LTE congestion in central London (new)<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage (managed)<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>High: Flu epidemic (managed)<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - ; - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels; - 20%<br>Medium: UPS Packages lost (managed)<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags: London, Supply Chain<br>High: Wifi unstable (managed)<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level; - 15%<br>High: Tube strike (managed)<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000<br> Impact<br>Probability<br>0 0 0 0 0<br>0 0 0 0 0<br>0 0 2 1 0<br>0 0 2 1 0<br>0 0 0 0<br>new<br>managed<br>1<br>5<br>Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive |
| 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. | |
| **Claim: 16** | |
| 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; | ALYNE 2;<br><br>Alyne \| Risk Management<br>Secure https://pre-prod-alyne.firebaseapp.com/risks?allRisks=true&view=risks<br> alyne<br>Risk Management<br>Stefan Sulistyo<br>alyne.com<br>Search Screen<br>Tracked Risks<br>6<br>Active Risks<br>6<br>Risks in selection<br>Impact<br>Probability<br>Risk Rating<br>0<br>Excessive critical Risks<br>0<br>Excessive very high Risks<br>Risks by Rating<br>Risk Exposure<br>Exposure development of selected Risks based on planned mitigation actions<br>Risk Status<br>1<br>5<br>new<br>managed<br>Number of selected Risks by current status<br>HR<br>IT<br>Munich<br>London<br>Supply Chain<br>High: LTE congestion in central London — new<br>Sometimes it is difficult to get a proper connection<br>High · Almost Certain · € 1,000<br>Comments<br>Stefan Sulistyo updated in risk rating 3 minutes ago<br>Write comment...<br>Medium: Elevator outage — managed<br>This will cause issues to deliver packages and people.<br>Medium · Very Likely · € 2,500<br>High: Flu epidemic — managed<br>Increased staff outages due to flu.<br>High · Very Likely · € 50,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Work from home options — Stefan Sulistyo - 31 Mar 2018 — - · - 25%<br>Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels · - 20%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>Medium: UPS Packages lost — managed<br>Packages have been lost in transit.<br>Medium · Very Likely · € 1,000<br>Risk Tags<br>× London × Supply Chain<br>High: Wifi unstable — managed<br>Possibly due to interference<br>Medium · Almost Certain · € 5,000<br>Mitigation Plan<br>Stefan Sulistyo raised this risk on 26 Mar 2018.<br>Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level · - 15%<br> Mitigation Task<br>Mitigation via Controls<br>Risk Accept<br>Close and Archive<br>High: Tube strike — managed<br>Transportation strike in London will cause people to not reach the office.<br>High · Very Likely · € 2,000 |
| 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. | |

**Note:** Total claims: 16 and Independent claims: 3

| **EXHIBIT H** | |
|---|---|
| **Quantar’s Preliminary Infringement Contentions** | |
| **US Patent No: 16/129,820** | **Accused Instrumentalities** |
| **CLAIM 1.** | |
| A system, comprising one or more networks comprising computing systems that are subject to a security policy, the security policy comprising breach parameters defining one or more events that are indicative of an electronic threat, the security policy breach parameters being associated with a remediation provision in a network security device policy for the computing systems and the network or networks; | |
| one or more data and traffic collecting devices, deployed within the network or networks, that collect entity information and monitor network data and traffic of the network or networks that is related to security information; | |

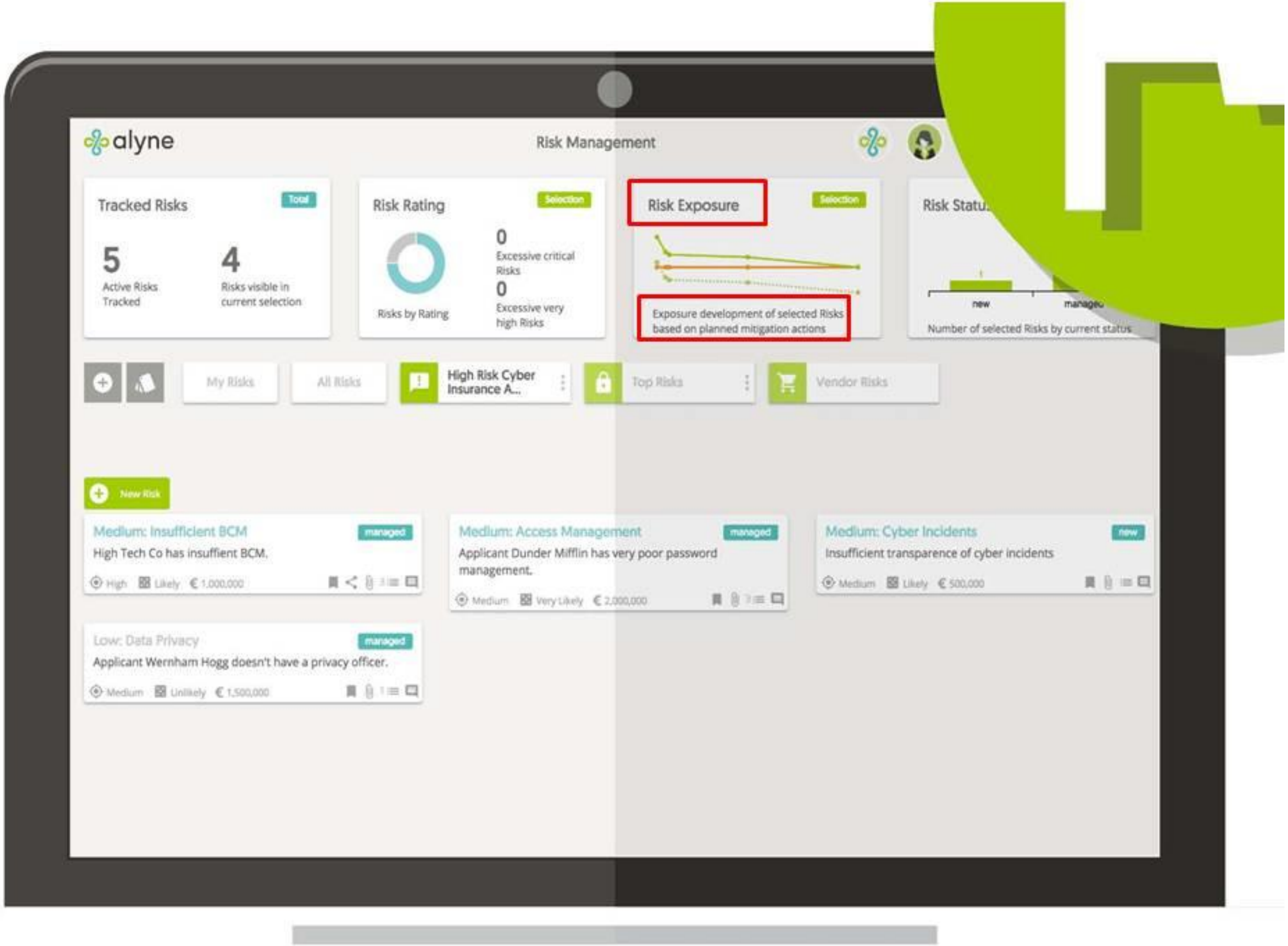
| | |
|---|---|
| samples network data and traffic and automatically detects occurrence of one or more of the events that are indicative of an electronic threat based on the network data and traffic; | |
| identifies electronic threats using a list of known threats stored in a database; | |
| produces observed electronic threat data, which includes a list of the observed electronic threats and their frequency of occurrence and stores the data in a database accessed by a threat assessment system that; | |
| automatically determines the breach parameters that apply for the one or more electronic threats that have been identified; and generates a remediation of network security device security parameters for the network or networks based upon predicted losses arising from the observed electronic threats. | |
| **CLAIM 16.** | |
| A method, comprising:<br>establishing security parameters for an entity, the security parameters defining one or more events that are indicative of an electronic threat, the security policy breach parameters being associated with a remediation provision in a network security device policy of the entity | |
| | |

| | |
|---|---|
| automatically detecting occurrence of one or more of the events that are indicative of an electronic threat; | |
| automatically determining the breach parameters that apply for the one or more events that occurred;<br>and | |
| causing a remediation of network security device security parameters determined based upon predicted losses arising from electronic threats. | |
| **CLAIM 20.** | |
| A system, comprising:<br>one or more data and traffic collecting devices deployed within a network that collect entity information and monitor network data and traffic of the network that is related to security information, the network comprising computing systems that are subject to a security policy, the security policy comprising breach parameters defining one or more events that are indicative of an electronic threat, the breach parameters being associated with a remediation provision in a network security device policy for the computing systems and the network or networks; | |
| a threat analyzer and threat assessment system:<br>automatically detects occurrence of one or more of the events that are indicative of an electronic threat based on the network data and traffic; | |
| | |

| | |
|---|---|
| automatically determines the breach parameters that apply for the one or more electronic threats; and generates a remediation of network security device security parameters for the network or networks based on predicted losses arising from the observed electronic threats. | |

# EXHIBITS

## ALYNE 1



alyne

Risk Management

Tracked Risks — Total

5 Active Risks Tracked

4 Risks visible in current selection

Risk Rating — Selection

Risks by Rating

0 Excessive critical Risks

0 Excessive very high Risks

Risk Exposure — Selection

Exposure development of selected Risks based on planned mitigation actions

Risk Statu

Number of selected Risks by current status

Medium: Insufficient BCM — managed

High Tech Co has insuffient BCM.

High · Likely · € 1,000,000

Medium: Access Management — managed

Applicant Dunder Mifflin has very poor password management.

Medium · Very Likely · € 2,000,000

Medium: Cyber Incidents — new

Insufficient transparence of cyber incidents

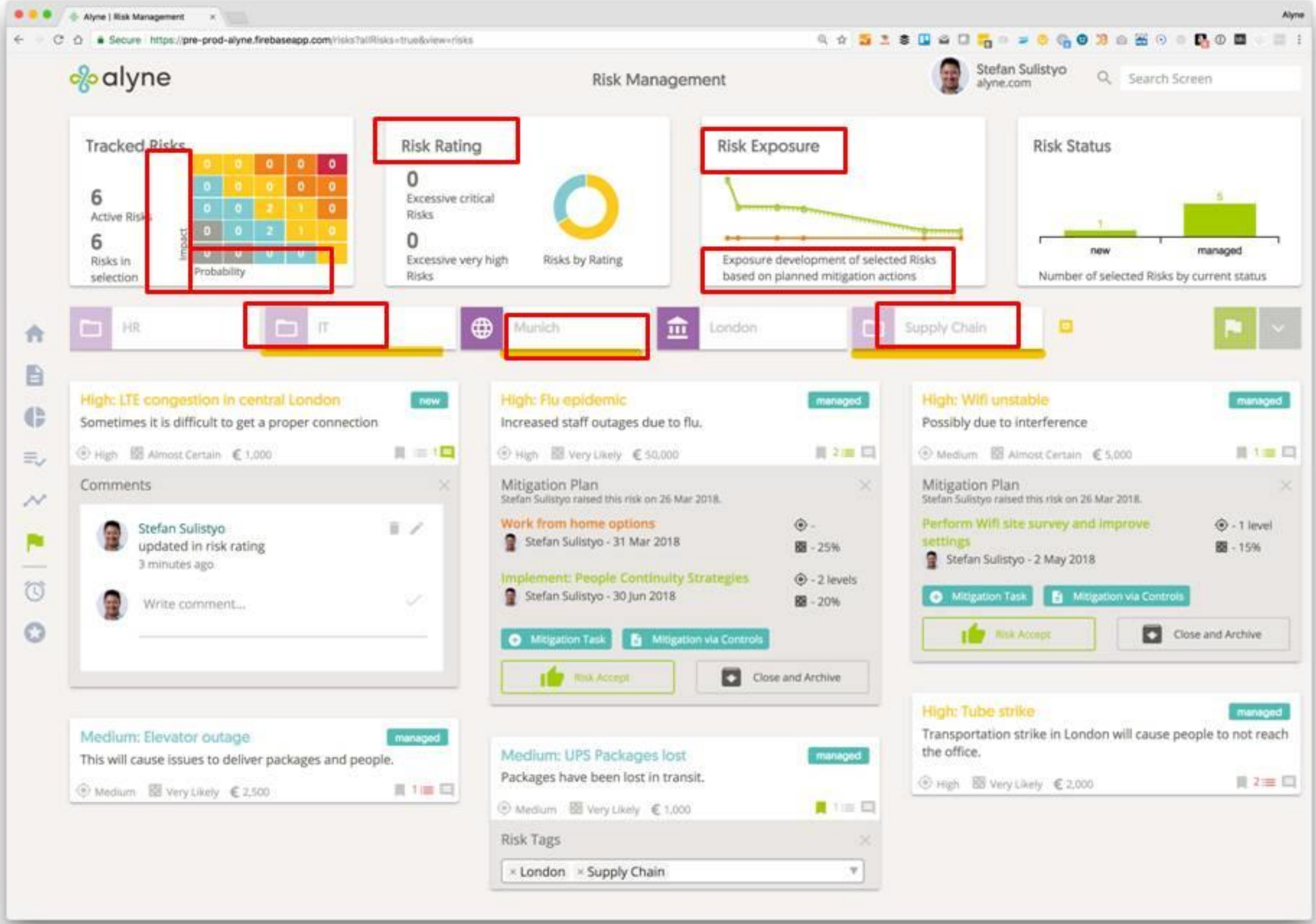
Medium · Likely · € 500,000

Low: Data Privacy — managed

Applicant Wernham Hogg doesn't have a privacy officer.

Medium · Unlikely · € 1,500,000

## ALYNE 2



Risk Management

Tracked Risks

6 Active Risks

6 Risks in selection

| | | | | |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 2 | 1 | 0 |
| 0 | 0 | 2 | 1 | 0 |
| 0 | 0 | 0 | 0 | |

Risk Rating

0 Excessive critical Risks

0 Excessive very high Risks

Risks by Rating

Risk Exposure

Exposure development of selected Risks based on planned mitigation actions

Risk Status

| new | managed |
|---|---|
| 1 | 5 |

Number of selected Risks by current status

High: LTE congestion in central London — new

Sometimes it is difficult to get a proper connection

High · Almost Certain · € 1,000 · 1

Comments

Stefan Sulistyo updated in risk rating 3 minutes ago

Write comment...

Medium: Elevator outage — managed

This will cause issues to deliver packages and people.

Medium · Very Likely · € 2,500 · 1

High: Flu epidemic — managed

Increased staff outages due to flu.

High · Very Likely · € 50,000 · 2

Mitigation Plan

Stefan Sulistyo raised this risk on 26 Mar 2018.

Work from home options — Stefan Sulistyo - 31 Mar 2018 — - ; - 25%

Implement: People Continuity Strategies — Stefan Sulistyo - 30 Jun 2018 — - 2 levels ; - 20%

Medium: UPS Packages lost — managed

Packages have been lost in transit.

Medium · Very Likely · € 1,000 · 1

Risk Tags

× London × Supply Chain

High: Wifi unstable — managed

Possibly due to interference

Medium · Almost Certain · € 5,000 · 1

Mitigation Plan

Stefan Sulistyo raised this risk on 26 Mar 2018.

Perform Wifi site survey and improve settings — Stefan Sulistyo - 2 May 2018 — - 1 level ; - 15%

High: Tube strike — managed

Transportation strike in London will cause people to not reach the office.

High · Very Likely · € 2,000 · 2

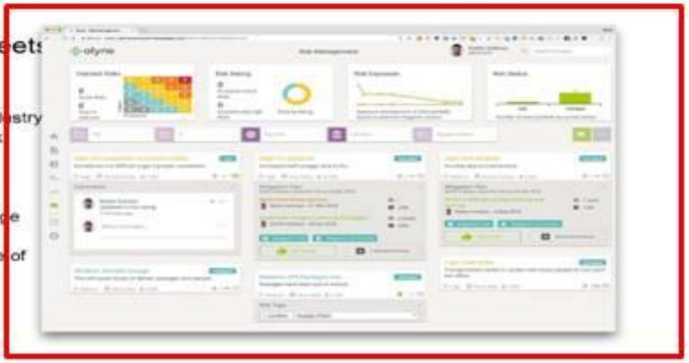
## ALYNE 3

Cyber Security, Risk Management and Compliance as a Service.

## Are you finding working with spreadsheets challenging?

Many organisations - especially in the financial services industry - are quite proficient in managing market risk and credit risk either due to regulatory pressure or business necessity. Operational Risk is traditionally treated less methodically.

Most organisations resort to various spreadsheets to manage their operational risk. In future this may not be enough, as regulators are focussing more on Operational Risk because of increasing complexity.



## Gain Transparency of your Operational Risks with Alyne

Alyne provides your organisation with a cost efficient and powerful toolset to create transparency around your **Operational Risks** and significantly reduces management effort.

Next Generation User Interface
Interact with a modern and user-friendly next generation interface that is as easy as using social media

Extensive Content
900+ Controls, ready to use, creating agility and faster implementation timescales.

35 out of the box; Standards, laws and regulations relating to InfoSec, Data Privacy (incl. GDPR), Operational Risk, Vendor Governance, Cyber Security

Enable & Transform Risk & Compliance Culture
Create an active risk culture, managing your risk and compliance at the speed of today's digital business.

Lowest TCO
Gather risk data for your entire enterprise cost effectively.

Security by Design
Cutting-edge web technology, implemented by security experts to create a highly secure and resilient SaaS offering.

Information Analytics
Leverage Information Analytics to align your risk to your business objectives, tracking risk mitigations and treatments

Instant Deployment
Alyne's SaaS Plattform solution can be deployed organization-wide in minutes