Vendor management system

Version 1 – June 7, 2021
DV2573: Decision Support Systems

Robert Mihaila (19990826-T119)[1], David Centellas (20000505-T032)[2], and María Peña (20000714-T161)[3]

[1,2,3]Blekinge Tekniska Högskola
[1]romi20@student.bth.se
[2]dace20@student.bth.se
[3]mapm20@student.bth.se

June 7, 2021

1 Abstract

This report covers an intelligent decision support system (IDSS), which handles an efficient and effective way to rapidly analyze the potential cyber-risks, and its solutions, of a company. The main risk analyzed is in the supplying vendor chain, the supplying vendor chain is the set of companies providing software or hardware products or components to the analyzed company.The system uses an if-else algorithm to evaluate the risk for a company to suffer an attack. This technique saves time and money on finding vulnerable points during the process of carrying out the product such that, instead of analyze n supplying companies,only 1 inspection is needed. The possible security problems are stored on a list with their possible solutions, in most of the cases, the solution given is a recommendation to change in the company, except in some cases the solution provided is not a specific solution, i.e. when signing a contract with a supply vendor, add a clause for them to check their security and provide you a product 100% secure. The report describes the problem domain and the implementation of the simulator prototype, showing how the system operates.

2 Introduction

The system´s goal to achieve is to promote a secure supply chain by the development of new solutions to empower the cybersecurity position of the company [1]. Therefore, enhancing resilience and creating a non-dependant environment will be its objective towards a secure supply chain. In the domain of cyber-risk industry, creating a framework to assess the issue of digital threats to an organization is always a challenge. The overwhelming amount of input data to consider makes it difficult not only to the framework itself, but to the organization´s committee to use a conclusive IDSS.

The aim of this project is the development of a system that efficiently helps evaluate the organization´s position on security standards. By using auxiliary frameworks such as NIST (National Institute of Standards and Technologies) [2] or COBIT (Control Objectives for Information and related Technology) [3], further identification has taken place to determine reliable criteria. This criteria will then be contemplated in the algorithm used, which offers a request response solution towards the data provided by the enterprise. It offers an instant output to immediately decide what strategic plans should be developed in the business. Moreover, the introduction of graphics, taking into consideration all companies in the database, creates a real-time solution mechanism to control the market trend and evolution. Identifying this trend is significant as continuous feedback into the algorithm will be valuable to its progression according to the market. In addition, it is also key towards companies, as they could consider strategic decisions based on the analysis of the industry as a whole.

3 Division of labor

We consider our work to be the same for all members of the group in terms of time, when realizing the project we divided the tasks so we could all work at the same time. The following solely outlines the main load of certain tasks conducted distinctly by each team member:

Forename	Surname	Project Duty*
Robert	Mihaila	A-H
David	Centellas	A-H
María	Peña	A-H

Table 1: Division of labor

A- Manager, **B-** Designer, **C-** Programmer, **D-** Documenter (report), **E-** Logger (team session events), **F-** Presenter, **G-** Viewer/reviewer (proof reading), **H-** Reviser (project revisions)

Tasks done for the IDSS final project:

I DB creation and data management issues

II Data graphics

III Algorithm

IV Connecting task I, II and III in order to do the graphics of our own data introduced

V GUI to display the output of tasks II and III

VI Form to introduce the new data of a company

VII Project presentation

VIII Power point to present the project

IX Documentation

4 Project analysis

4.1 Background

The vendor mangement system IDSS project is a system which tries to evaluate the digital threats an organization can be susceptible for. Consequently, it analyzes and provide an outcome with the cyber-risk mark it obtained. These outcome promoted are supposed to help the enterprise show their current cyber-risk state and act accordingly with some predefined solutions. The criteria specified will be developed according to the previously mentioned frameworks (NIST and COBIT). It will act as the backbone of the IDSS system to promote its decisions and best practices in the supply chain ecosystem. Further elaboration will be developed to show the intelligence of the data visualized. This is clearly visible in the implementation of different graphs representing the indexed enterprises. As an example, being able to see the trend relating the employees awareness and the cybersecurity investment could be a determining point in the enterprise´s cybersecurity strategy. This charts are the addition to the algorithm created, which will measure the cybersecurity risk obtained for an specific company, deriving in interesting solutions that will change according to the input data provided by the company. In a smaller but not less important scale, we include an antivirus section that could be manually updated according to different rankings on the internet.

4.2 Problem definition

1. There is normally an uncontrolled supplying vendors surface.
2. The data addressing security in a company is not properly structured.
3. Both employers and employees tend to have a low cybersecurity awareness level.
4. Parameters are defined as follows:
    - **Company name,** The legal name of the petitioner enterprise.
    - **Crypto mechanism,** The cryptographic mechanism of the petitioner enterprise.
    - **Company data update,** The last time the information of the petitioner company has been updated in the database.
    - **Product update,** The last time the product of the petition company has been updated.
    - **Employee awareness,** The average employee awareness the petitioner company has been updated.
    - **Number employees,** The total number of employees the petitioner company has.
    - **Annual revenue,** The total revenue the petitioner company acquires in a year
    - **Cybersecurity investment,** The money dedicated to cybersecurity parameters
    - **Number devices,** The number of devices (Datacenters, servers, workstations, mobile phones, etc...) the petitioner company possesses.
    - **Number audits,** The number of general cybersecurity controls to check the success of the cybersecurity implementations the petitioner company performs.
    - **Cybercrisis team,** The existence of an internal or external cybercrisis team, in case an incident appears, in the petitioner company.
    - **Contingency plan,** The existence of a plan to recover from any possible incident by the petitioner company.
    - **Signed cybersecurity requirements,** The existence of agreements with the supplying vendors to fulfill specific security requirements over the products they provide the petitioner company with.
    - **Role validator,** The existence of a person or team that ensures the validity of the supply chain with the corresponding vendor in the petitioner company.
    - **Antivirus id,** The antivirus the petitioner company possesses, formatted to the most known antivirus which has their own section based on their performance ratings.
    - **Two factor authentication,** The existence of two factor authentication in the authentication methods of the petitioner company.
    - **Isolated backups,** The existence of isolated backups to fight ransomware and other significant threats in the petitioner company.

  - **Data risk,** The level of importance of the data the petitioner company possesses.
  - **Supplying vendors,** The number of supplying vendors the petitioner company has.

5. **Parametric adaptations:** As expected, the antivirus id will refer to an internal antivirus referenced in the database. This antivirus are sorted following different criteria which are:

   - **Id Antivirus,** The name of an antivirus
   - **Overall efficacy,** The total efficacy of an antivirus to protect against threats.
   - **User mark,** The user experience and perception of the antivirus in the protection of threats.
   - **Price,** The price of the antivirus.

   Another adaptation will be followed in reference to the Data risk parameter. Internally they are sorted with numbers as follows:

   1 Low.

   2 Medium.

   3 Critical.

4.3 Problem objectives

- Detect risk associated with supplying vendors.
- Reduce risk.
- Identify security requirements for the vendors of the assets.
- Analyze input data to calculate risk percentage of cyber-attack.
- Suggest specific solutions based on the input data introduced.
- Finalize results showing the solutions to the company client.
- Graphs:
  - Make statistics of the data entered together with the rest of the db.
  - Representing statistics by means of graphs.

4.4 Problem solution

For the resolution of the problem we collect the data, analyze it and calculate the best result, for that we followed these steps:

1. Define the set of data we need to know in order to properly analyze the risk associated with that company.
2. Ask the data to the company.
3. Insert data into database.
4. Recalculate graphics.
5. Assign a risk associated to each value introduced.
6. Sum all previously analyzed data to define the company's risk.
7. Detect the most fragile points where they can attack.
8. Decide which problems are worth solving based on the type of data the company handles, the budget currently invested and the money it can afford to invest.
9. Give the associated solution attached to each problem.
10. Display the risk percentage and our suggest solutions on the web page.

4.5 System criteria

The system display a object type company with its assigned values, this is the data the petitioner has introduced in the form (company name, crypto mechanism, company data udate, product update, employee awareness...). This has already been saved on the database. The algorithm, first of all, will determine how much money of the annual revenue the company should invest on cybersecurity, this will be determined by the type of data the company handles:

1. Low: Only low-risk personal data such as name, email or phone number.
2. Medium: Sensitive personal data as the address where the customer lives.
3. Critical: Critical information that should not be disclosed because it is not public, such as criminal or medical records.

Normally when a company processes data of one type, it also processes all lower types, so we will always assign the highest type for greater security.

We have assigned a 13%, 19% and 26% respectively. This values comes from a previous study that we have done with other company cases based on the suffered attacks and the annual incomes of the company. We considered risk and benefits in order to be able to find a middle point where the company do not loose more money that they can afford but they lower to the minimum possible the risk.

After assigning the percentage that we consider should be invested in security, we calculate the percentage currently invested.

In the following formula is specified how we calculated the actual investment percentage comparing it to annual revenue and actual investment in security:

$$Investment = \frac{Annual_r}{Annual_i} \times 100 \quad (1)$$

Once we know how much the company invests in cybersecurity, the system will calculate the percentage that can still be invested, i.e., what the company should be investing but is not.

$$Available_i = Desired_i - Actual_i \quad (2)$$

The algorithm will always work with the available investment and in percentage, since this way the data will be more in line with reality. In the end, the costs of a new antivirus or two-factor authentication are not the same in a company with a volume of 100 million euros as in a company with a volume of ten thousand euros. For this reason, we believe that managing the data as a percentage of what the company can and must invest will be more accurate.

Once the system has all the data it needs, the analysis begins. Each data entered has a cost, in percentage, associated with it. So the system would check if the company has a certain quality and if it does not, it would be added to a list of qualities to improve.

The qualities we have considered as the most important are:

- Contingency plan
- Isolated backups
- Good antivirus

The system has a cost associated of 2, 8 and 4 respectively. The algorithm will check this in order to prioritize them rather than the rest.

The algorithm will continue checking in the following order:

- Ciphered communications
- Audit number
- Two factor authentication
- Cybercrisis team
- Supplying vendors cost

To analyze the problems, the algorithm will check if the company has implemented this requirement. If not, it will check the percentage of investment that can still be invested with what it will cost to implement the functionality. If it is possible because there is still that amount of money available, it will be added to the improvements, otherwise it will move on to the next one. This is done because it is not an If-Else algorithm but an If-If algorithm, so no functionality is excluded unless there is no money to invest in it. The reason for this is that in many cases it is not possible to invest in an important functionality, however, any security improvement counts. If there was a less important but cheaper functionality it would be done.

Once the data has been analyzed, the system will extract the percentage of risk of suffering a cyber-attack.

As before, when analyzing whether a requirement could be carried out or not, each functionality has an associated value. It will check whether the company complies with the requirement and if not, the value associated with that risk will be added.

Once all the values have been calculated they are returned to the calling program so that they can be printed on the web page.

4.6 Swot analysis

We have conducted our SWOT analysis (strengths, weaknesses, opportunities and threats) of the project and presented in the following table:

Strenghts	**Weaknesses**	**Opportunities**	**Threats**
Risk awareness	Missing machine learning algorithm	More cyber-security investment	Sensitive information in the DDBB
High number of requested criterias	No continuous integration system	Emerging need for cybersecurity risk analysis	
Visual data display	Running in local		

Table 2: Project SWOT analysis

5 Project design

5.1 Centralized architecture

The architecture of the Vendor Management System IDSS consists on a frontend web interface on top, relying on a backend which orchestrates both the frontend display and the connection towards the storage section, establishing its relation up to the user interface prompted in the web.

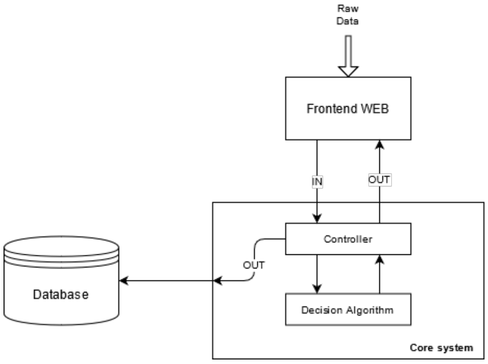

Figure 1: Centralized Architecture

This is illustrated in *[Figure 1]*, where we could see the two components, the algorithm and controller as the "core system" of this architecture. Here we consider the IN raw data towards the front-end WEB, being the input data provided by the user to create the desired enterprise. As well, we consider two movements OUT of this "core system". One is directed into the database to introduce the new value for further metrics. The other movement returns to the front-end after being evaluated in the algorithm component, which will return the values to be displayed in the web page.

5.2 Overall architecture

The overall architecture of our system has three important components: STS Framework[4], the data base[5] and clicdata[6]. The design consist of users (companies) interacting (filling a form) with our web page (running thanks to STS). In addition, STS runs at the same time our java code implementation that takes all the input data and saves it into the data bases. At the same time, the data is analyzed by the algorithm, which generates an output. This output is showed to in the web page as advises and a risk percentage. In the web page is also displayed some general statistics about the companies in the data base. This information is given by clicdata, which is linked to the data base. A layered architecture composed of use-cases and activities is given in *[Figure 2]* and *[Figure 3]*, respectively, and in the following subsections.

5.3 Use-Case Diagrams

An overview of the use-cases can be found in *[Figure 2]*. The actor in our use-case diagram would be the company that introduces the data on the website and its able to perform the case of use, analyze the data. Right now everything else that happens is included when the company press "analyze".

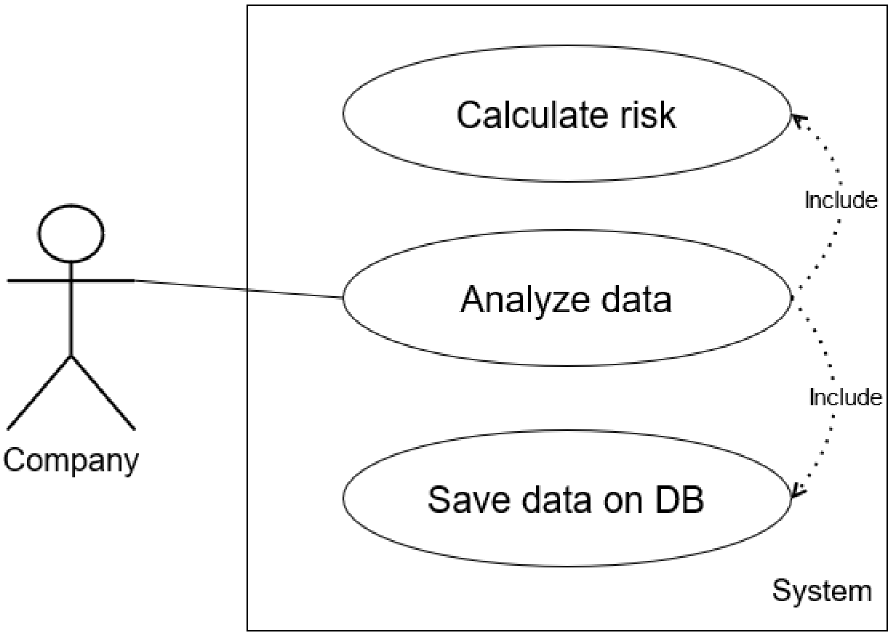

Figure 2: Use case diagram

A possible work for the future would be separate these three cases but right now we have consider that the best option is to give the customer all the information that he/she wants. When the program analyze the data it always send the new information to the database and calculate the risk because most of the information that we need to analyze the data is also used to calculate the risk. This way we optimize time and resources calculating both functionalities at the same time.

5.4 Activity Diagram

The *[Figure 3]* is an Activity diagram with swimlane, each partition represents one actor of the system, the user would be the representative of the company designed to fill out the form. He/she would open the web and introduce all the data required in the form, once the button to analyze is pressed the system will create a object type company with all the data. It will analyze the data and store the information to afterwards show the results on the web for the client.

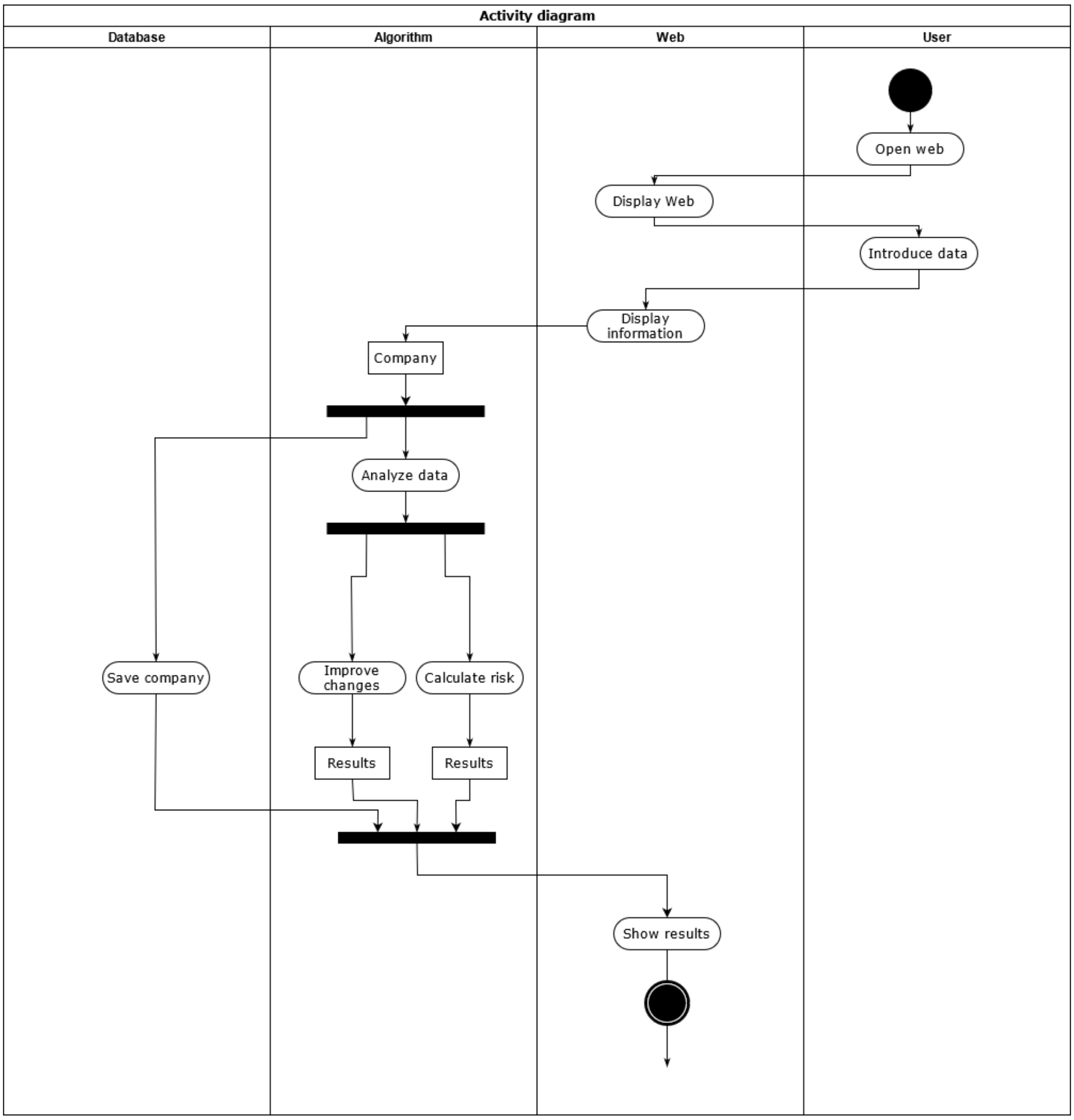

Figure 3: Activity diagram

6 Project implementation

6.1 Analyzer code

The *[Figure 4]* and *[Figure 5]* describe the process to analyze the data. The first one will prepare the money values in order to set the percentage values needed in *get_possible_improvements()*. It will be the program called from the outside of the class because it will also return the final result.

```java
public String[] analyze_data(){
    int ideal_investment_percentage = define_investment_percentage(data_risk);
    float ideal_cybersecurity_investment = (ideal_investment_percentage * total_incomes)/100;
    List<String> changes;
    if (this.cybersecurity_investment < ideal_cybersecurity_investment){
        float actual_investment_percentage;

        if (this.cybersecurity_investment != 0 ) {
            actual_investment_percentage =(float) (this.cybersecurity_investment/this.total_incomes)*100;
        }else{actual_investment_percentage = 0;}

        System.out.println("Data risk: "+this.data_risk+" Total incomes: "+this.total_incomes+" cybersecurity investment: "+this.cybersecurity_investment+" idel investment "+
        ideal_cybersecurity_investment+" "+ideal_investment_percentage+" actual investment percentage "+actual_investment_percentage);

        changes = get_possible_improvements(ideal_investment_percentage - actual_investment_percentage);
    }
    else{changes = new java.util.ArrayList<>(Collections.emptyList());}
    String[] array_changes = new String[changes.size()];
    int i;
    for (i=0; i<changes.size() ;i++) {
      array_changes[i]= changes.get(i);
    }
    return array_changes;
}
```

Figure 4: Data analyzer

First of all, the program will check if the company can afford to invest more money in cybersecurity, if they are already investing the same or more amount of money than what we recommend, we will not suggest anything. As more investment is more security.

After this, we define the ideal percentage to invest and the actual investment percentage.

As, we can see, the object return from *get_possible_improvements()* is a list of String but the web page was not able to read that, so it had to return an array. The array is defined on the loop.

```java
public List<String> get_possible_improvements(float percentage_budget){
  List<String> improvements = new java.util.ArrayList<>(Collections.emptyList());
  double cost = IdealDataValue.get_contingency_plan_cost();
  if (!company.isContingency_plan() && percentage_budget > cost) {
      percentage_budget = (float) (percentage_budget - cost);
      improvements.add("A contingency plan - in case an attack occurs the company would be able to fix it with less public damage and faster. The cost should be a "+cost+"% of the investment in security");
  }
  cost = IdealDataValue.get_isolated_backups_cost();
  if (!company.isIsolated_backups() && percentage_budget > cost){
      percentage_budget = (float) (percentage_budget - cost);
      improvements.add("Frequently isolated backups - if for some reason the company lost its data because, for example, a problem with a server, it is easy to recover from the last backup. The cost should be a "+cost+"% of the investment in security");
  }
  cost = IdealDataValue.get_antivirus_cost();
  if (is_not_best_antivirus() && percentage_budget > cost){
      percentage_budget = (float) (percentage_budget - cost);
      improvements.add("Adquire a better antivirus - we recommend you McAfee. The cost should be a "+cost+"% of the investment in security");
  }
  cost = IdealDataValue.get_ciphered_communication_cost();
  if (!company.isCiphered_communications() && percentage_budget > cost){
      percentage_budget = (float) (percentage_budget - cost);
      improvements.add("Ciphered communications - protects your data much better. The cost should be a "+cost+"% of the investment in security");
  }
  cost = IdealDataValue.get_audit_number_cost();
  if (is_not_enough_audits() && percentage_budget > cost){
      percentage_budget = (float) (percentage_budget - cost);
      improvements.add("Increase the number of audits to at
 least 3. The cost should be a "+cost+"% of the investment in
  security");
    }
    cost = IdealDataValue.get_two_factor_authentication_cost();
    if (!company.isTwo_factor_authentication() &&
 percentage_budget > cost){
        percentage_budget = (float) (percentage_budget - cost);
        improvements.add("Two factor authentication - make the
 attackers really hard to enter in your system when a
 phishing attack occurs. The cost should be a "+cost+"% of
 the investment in security");
    }
    cost = IdealDataValue.get_cybercrisis_team_cost();
    if (!company.isCiphered_communications() &&
 percentage_budget > cost){
        percentage_budget = (float) (percentage_budget - cost);
        improvements.add("Cybercrisis team - the team that will
  solve an attack problem as fast as possible and minimizing
 the damage. The cost should be a "+cost+"% of the investment
  in security");
    }
    improvements.add("Reduce supplying vendors number - with
 less suplying vendors less risk of an attack in the
 supplying vendor chain");
    System.out.println("Still left "+percentage_budget+"% of
 the budget");
    return improvements;
}

```

Figure 5: Define possible improvements

The program check is a field is *True* or *False* in case of booleans, and the expected input in case of integers. When the value is not the expected one, the field will be added to the list with its corresponding solution. This way, the return value is a list of String ready to be displayed.

The *[Figure 6]* describe the code that analyze the risk of suffering an attack of the company.

```
public float company_risk_percentage(){
    int risk = 0;
    if (!company.isContingency_plan()){
        risk = risk + 20;
    }
    if (!company.isIsolated_backups()){
        risk = risk + 20;
    }
    if (is_not_best_antivirus()){
        risk = risk + 20;
    }
    if (!company.isCiphered_communications()){
        risk = risk + 14;
    }
    if (is_not_enough_audits()){
        risk = risk + 14;
    }
    if (company.isTwo_factor_authentication()){
        risk = risk + 6;
    }
    if (company.isCybercrisis_team()){
        risk = risk + 6;
    }
    return risk;
}

```

Figure 6: Risk calculator

The code above check if every field is correct, in terms of security, and if its not it will increase the number assigned to the risk. This means that if none of the values were correct, the risk would be 100% and otherwise 0%.

6.2 Database

We could establish the database in use as a multi-purpose database. Its contents are wide yet linked and coherent. We could clearly distinguish three consistent purposes:

I The main purpose is set to store and structure the data of the petitioner company. The table in which the companies are inserted will then be used by an external component named Clicdata.

II A secondary purpose that provides scalability and adds functionality to the system is the collection of antivirus. The best antivirus is selected for the report from the analysed data.

III A developing purpose is the relation of the companies with the supplying vendors. Nowadays we consider that adding the information of all supplying companies could be time-consuming and consequently inefficient. We strongly encourage all companies to perform the questionnaire as data will become reliable with the market trend and will show conclusive graphs. In adittion, this relation.

Due to the previous motivations, we could clearly state that the system, and specifically the frontend and external component, heavily relies onto the database itself. Accordingly, the database happens to be a key component of the system, as structuring the data of the petitioner company was one of the main objectives of the IDSS.

6.3 Model

The domain knowledge used in the model has been thoroughly discussed. As the environment data is wide and sometimes fuzzy, the selected criteria is intended to be clear and conclusive towards the expected IDSS. Its creation, as previously mentioned, contemplates creating a quick and effective system to calculate the cyber-risk of the petitioner company. As previously mentioned, the graphics displayed in the web represent a uniform set of results that could be either validated or compared with in further studies. For example, a survey that will assess the employee awareness of the different companies in the software engineering industry. This survey could compare the employee awareness estimated in software engineering in front of the general industry data.

6.4 Simulation Results

The main simulation results are on last instance visualized in the frontend webpage. Previously, this dataset has been considered both in the external component and in the core system and will both prompt the result in the unique interface provided. The main aim of this data to be displayed is for the manager of the petitioner company. Who will set different strategies according to the companies budget, business plan and of course, this decision support system to reduce the cyber-risk their company possesses.

7 Evaluation

7.1 Verification and Validation

In order to verify and validate our results, we created an experiment which involves different companies, with the purpose of checking if the advice we give are actually useful. The most influencing parameter that we took into account during the development of the algorithm was the employees awareness. Other important criteria are if the company has back ups, if it has a good antivirus or if there is created and deployed a contingency plan. Thus, we filled the form with some inputs that we considered "not really secure" as it could be a low employee awareness (< 75), or a 'no' as the answer to the question about if the company has recent back ups. As we expected, the analysis result was that ,currently, this company has about 88% of cyber-risk. We also got some advises as for example:

- *"Two factor authentication - make the attackers really hard to enter into the system when a phishing attack occurs. The cost should be a 18% of the investment in cyber security"*

- *"Frequently isolated backups - if for some reason the company lost its data because, for example,a problem with a server, it is easy to recover from the last backup. The cost should be a 8% of the investment in cyber security"*

- *"Acquire a better antivirus - we recommend you McAfee. The cost should be a 2% of the investment in cyber security"*

Taking this into account, afterwards we filled again the form with exactly the same data but with the improvements that the web page suggested. The aim of it was to check if the algorithm works properly and gives to us a valid and reasonable result. And it happened, the risk result we had after doing the suggested changes was better than we expected: 40% of cyber-risk, which is less than a half of the first analysis.

With this analysis we concluded that our algorithm works as we expected. Also, the changes that it suggests are important ones that really helps to protect the company in terms of cybersecurity.

8 Future work

Our project has a very powerful base on which we would like to continue developing and advancing. Currently, our vendor management system provides a set of solutions to a specific company, in base on its own input data. For the future, we would like to do a much more in-depth analysis and give companies a percentage of risk as accurate and close to reality as it is possible. To do so, we have developed several proposals to be implemented:

- **Application web deployment:** Currently, the web is running on local host. The objective would be to deploy, the web page and the entire backend, on a server with a proper domain. So that companies from all over the world can access to it.

- **A machine learning algorithm:** The logarithm that is implemented right now, is an "if / else" algorithm. In order to give more accurate results to our clients, we have considered to implement a machine learning algorithm. More complex, more accurate and with a proper training, we truly believe in giving the best solutions to each company.

- **Personalized visual outcomes:** The easiest way to show people the final result is making graphs. Trying to read only text and numbers in the final results could be hard and exhausting. Thus, the solution is showing that data with visual graphs; easier to understand, faster to read and they twice as convincing.

- **Login for companies:** One of our final objectives is having constant customers. To reach so, the web application need a register/login form. With these functionalities implemented, we also would be able to give some stats about their improvement during the time they trusted as and our work.

- **Risk analysis based on suppliers:** To do a deep analysis about the risk that a company could have, not only the data about that company is necessary. We also need their supplying vendors. Analysing the risk that those suppliers have, and matching it with the risk that the main company has, we would be able to a calculate a really precise risk percentage. At the same time, and thanks to the machine learning algorithm, the advice would be more specific and personalized giving to the clients what they need at the proper moment.

9 Conclusions

In this project we have managed to create a continuous environment system. It connects a database (MySQL) with a web page (the Vendor Management System) and a web site (clickdata) to make accurate graphics taking into account different data and calculated statistics. As well as the connection between the web page and the SpringBoot Tool Suite Framework running in the background in order to analyze the input data. Java application was connected with the data base as well with the objective of either add new data into the data base or to refresh some of the old ones. The final project is a complete Decision Support System for the companies that uses it. We managed to implement the NIST[2] and COBIT[3] frameworks in a more dynamic and easy-for-the-user format.

> “Work smarter, not harder.”
>
> *Allen F. Morgenstern*

References

[1] NIST: National Institute of Standards and Technology. *BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT.* https://www.nist.gov/system/files/documents/itl/csd/NIST_USRP-FireEye-Cyber-\SCRM-Case-Study.pdf

[2] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[3] ISACA. *COBIT® 2019 FRAMEWORK: INTRODUCTION METHODOLOGY.* https://spring.io/tools

[4] Sping. *Spring Tool Suite.* https://spring.io/tools

[5] MySQL. *MySQL Database.* https://www.mysql.com/

[6] ClicData. *ClicData DashBoards.* https://www.clicdata.com/