15. Exercise: Cost of incident handling

15.1 What will you learn?

In this exercise you will:

- learn how to estimate the costs of security incidents;
- gain practice in such evaluations and in substantiation of the security investments in a budgeting process.

15.2 Exercise Tasks

During this exercise you will analyse five types of incidents (spam, virus, DDoS, customers' data theft, botnet identified) that may occur in two types of institutions (a commercial company and a college, hereafter called 'entities'). Each of the incidents will cause substantial losses at each of the entities. Their monetary values will be estimated. After the frequencies of these incidents' occurrences are measured, the total expected loss in a unit of time will be calculated. The resulting numbers will show how much money is at risk and how much can be saved if a security incident happens and the company is properly prepared.

The two analysed entities are an Internet (online) store and a college, both comparable in size with around 100 employees. Being of similar size, they have similar yearly costs. These costs must be covered by the gross margin of a merchant company (i.e the revenue less the cost of goods sold) or by the revenue itself (if the cost of goods sold is negligible, like in the case of the college).

15.2.1 Terminology

Cost of goods sold – the price that the company pays for all the goods sold during the fiscal year.

Gross margin (also called **gross profit margin** or **gross profit rate**) – the difference between revenue and cost before accounting for certain other costs. Generally, it is calculated as the selling price of an item, less the cost of goods sold (production or acquisition costs, essentially).

Overhead – the term here used for all costs borne by the entity besides the personnel costs.

Revenue (also called **turnover**) – the annual sum of all net invoices issued by a company i.e. the total net price (without value added tax – VAT) of all products sold during the fiscal year.

ROSI (Return on Security Investment) – is the ratio of money saved or lost (whether realised or unrealised) on a security investment relative to the amount of money invested.

Task 1 ***Describe the working environment***

The exercise is based on a spreadsheets workbook, where the data associated with the security incidents have been filled. Most of the exercise will comprise the further discussion and modification of the workbook and a discussion of the results.

The currency used in the workbook is EUR (euro).

The workbook, called calculator, is placed in the working directory on the Virtual Image. It is located at: */usr/share/trainee/15_CIC/adds* and is given in two formats:

- *'Exercise 15 Calculator – CIC'* in Microsoft .xlsx format;
- *'Exercise 15 Calculator – CIC Open'* in open .ods format.

It consists of eight spreadsheets:

- assumptions and general information;
- five analysed cases;
- comparison;
- ROSI calculation.

Please open the Assumptions spreadsheet and fill/alter the following fields:

1. The employment structure of the Internet store (cells D5 to C9) and of the college (cells G5 to G9)
2. Their average yearly gross salary (cells E5 to E9 for the store and cells I5 to I9 for the college)
3. Number of students in the college (cellG12) and their yearly tuition (cell I12)
4. Number of average employee's working days in the entity in your country (cell C17). Generally it is the result of the following simplified calculation:
   52 * 5 (number of working days during 52 weeks of year)
   minus average number of public holidays in your country (typically between 8 and 14)
   minus average number of days of annual leave (typically in Europe between 20 and 26 days)
   minus average amount of annual sick leave in the entity
5. Internet store's yearly revenue (cell C15) and average gross margin (cell C16)
6. Overheads are to be entered in cells C18 and C19 for the store and cells G18 and G19 for the college:
   a. in row 18: all the costs associated with salaries (social security, insurance premium (if paid by employer), superannuation (if paid by employer), leaves, trade-union dues (in part that is paid by an employer) in relation to the total salary costs
   b. in row 19: all other costs borne by the entity besides total personnel costs and cost of goods sold (COGS) i.e. subcontractors' costs, rents, supplies, amortisation and depreciation, financial costs, etc.

All the variables in this spreadsheet are named in the workbook to facilitate your understanding of the formula.

In this exercise we will be calculating losses and not only direct costs to the company. Among the college's losses one should take the students' losses into account. They can be estimated based on the students' tuitions and they have also an indirect impact on the college. Among other losses you, the training participant, should include such losses as loss of know-how, reputation and even loss of competitiveness (Ponemon Institute study, 2011).

15.2.2 Task 2 Analyse the incidents

Incident 1: Spam

In the second spreadsheet there is a simple analysis of the spam costs. The entity is being flooded by spam. The filtering system is almost perfect: only a small fraction of the spam gets through the employees' mail boxes. Fill the following cells:

1. *the percentage of the spam mail that gets through the filtering system (cell G4);*
2. *the time used by an average employee to recognise it as a spam and delete it (cell G5).*

Please, remember the following.

- *The approach to spam is individual: some employees actually read it, others react to each mail system alert and delete it, still others have created and configured their individual trash bin, which they review and clean once in a while.*
- *The process of recognition and deletion should include the time in which the employee's attention is diverted from his/her current work, the process of recognition, and of deletion/cleaning, and the time required to return to his/her current work.*

The loss is significantly greater in the case of a college, since all students are also affected by the spam. Among the costs one has to take into account are also an increased telecommunication throughput and the use of the mail server's processing power to transmit and process the unwanted mail.

Incident 2: Virus

A percentage of entity employees were victims of a virus attack. The virus destroyed a number of days' work of these victims and meant that their systems had to be reinstalled. Please, fill the following cells:

1. *percentage of employees' computers affected (cell G3);*
2. *number of workdays lost by each of the affected employee (cell G4);*
3. *time (in minutes) to clean-up (and reinstall) one computer (cell G5);*
4. *percentage of the IT staff taking part in the problem recognition and cleaning processes (cell G6);*
5. *time (in hours) to recognise the problem and find a solution (cell G7).*

Additionally, as a result of the virus attack, the systems had to be reinstalled. In addition, a large number of students, whose computers were also affected, took up the consultation time of the IT Department, so a number of work days of the IT staff (cell G8) was required to deal with the problem.

Incident 3: DDoS attack

The entity has been attacked by DDoS attack.

Please enter the following information in the stated cells.

1. *The duration of the attack in hours (please, enter value into cell G3). For simplicity it has been assumed that the attacked started at midday on Monday (i.e. if your work-day is 9.00–17.00, then the attack started at 13:00). All employees and students work in one-shift mode, while the Internet store's customers place orders evenly round the clock. Hence, if the attack lasts 18 hours, only one-half shift is affected, while three-quarters of a day of sales is affected.*
2. *If there are no orders, a large proportion of the company's employees sit idle or do some maintenance jobs. Please enter the percentage of employees impacted and the level of their efficiency during the attack. Impact differs: the Internet store relies heavily on the attacked web site, whereas for college employees, daily activities are almost untouched by the attack.*

   Please enter these numbers in cell F5 and cell F6 for the Internet store and cell H5 and cell H6 for the college. The college does not rely so heavily on its web site, so the number of the college employees affected will be smaller. However, if the college offers some forms of distance learning, such a DDoS attack can significantly hinder the e-learning process for its duration. Please enter the percentage of students participating in this form of learning (in cell H7).

   Additionally, due to the loss of confidence, a percentage of potential customers and students have changed their minds and placed orders or enrolled elsewhere. Please, enter this percentage.

Incident 4: Data theft

Data theft, if it concerns the customers' or employees' personal data, may cause a need to pay the victims compensation (for example after a class action suit against the entity or as a result of contractual obligations). If contractual penalties or court sentences awarding the compensations/damages exist, they can amount to security breaches having huge costs. Here a class action against the entity due to the partial data base breach containing personal data caused heavy penalties for the entity. Please enter the number of victims, whom the entity must pay (cell G3) and the amount to be paid to each of them (cell G4). Please enter the amount of time of top management (cell B6) and lawyers (cell B7) and the external legal fees (cell B8).

Additionally, due to the loss of confidence, a percentage of potential customers and students have changed their minds and placed orders or enrolled elsewhere. Please enter this percentage in cell G9.

Incident 5: Active botnet member identified containing and distributing offensive content

Law enforcement agency (LEA) officers entered the entity's premises and seized a number of computers. This action has caused a general commotion among the employees for half a day. Please, enter the number of employees who were not working (or not efficiently working) for this time (due to the above commotion and due to other reasons caused by the LEA officers' performing their duties) in cell F7 and their average efficiency compared to normal (in cell F8). As a result of this action, the IT department lost and/or had additional work for of a number of workdays, which should be entered in cell F9. The same applies to for lawyers – cell F10 – and top management (cell F11).

The entity had to immediately buy replacement equipment for EUR 30,000 and wait for delivery as the seized equipment would stay at the prosecutor's office for a number of months. Afterwards, although these machines will still be useful for backup and alternate site purposes, their value will be negligible.

Some employees would be arrested/interrogated; that process additionally may cause interruptions in everyday work processes.

15.2.3 Comparison and conclusions

This spreadsheet compares the results for the Internet store and the college. Please, enter the expected frequencies (*ARO* in row 8) of each of the considered incidents. Use your intuition and experience, remembering that:

- for cases of spam, the frequency should be 1 (per year) as a this case is considered an everyday problem;
- DDoS attack happens much more often in the business (especially e-commerce) environment than in academia, where – if it happens – it generally has fewer consequences.

The results concern only five out of many possible security incidents, each of them carrying a significant risk of loss. As many as possible should be considered, for all of which the expected Annual Rate Of Occurrence (*ARO*) is non-negligible.

The obtained Annualised Loss Expectancies (*ALEs*) can be compared to the planned budgets or investment plans, addressing each of the probable risks. There are solutions that address a number of possible kinds of incidents. Their return on investment analysis should include the sum of all relevant ALEs.

15.2.4 Return of security investment (ROSI) calculation and discussion

Let us consider the decision whether to buy an additional security appliance for the Internet store and for the college. The numbers are given by the instructor.

The last worksheet of the workbook calculates the efficiency of the mitigation measures by reducing Annual Rate of Occurrence (*ARO*) according to the students' experience and therefore reducing the Annual Loss Expectancy (*ALE*) and Total Annual Loss Expectancy (*TALE*). Students should propose several mitigation methods and try how much in their opinion it could reduce *TALE*.

The formula behind the *ROSI* calculation, realised in the workbook, is the following: Savings due to cyber security means implemented – Solution Cost) / Solution Cost

The given mitigation method is effectively decreasing the *ARO* of each of the considered types of incidents. However, each of the ARO_i (and consequently ALE_i) is decreased by a different factor, X_i. Therefore, one has to calculate the change of *TALE* by multiplication of individual value of ALE_i by the corresponding decreasing factor X_i and then summing the products. This sum, multiplied by the number of years of the mitigation methods' effectiveness, *N*, can be compared with the mitigation method cost (investment). If the saving is larger than the cost, the investment is justified. The relative benefit and comparison between the methods should be performed using the ROSI parameter, which shows the savings volume compared to the investment.

15.3 Conclusion and lessons learned

The CERT team should be aware of the monetary values of the incidents and their expected occurrence probabilities (frequencies). The entity's management will accept the budgets for the mitigation tools not only if the proposed investments are justified, but also if the CERT team proves that the proposed solutions offer an optimal cost/benefit ratio. Therefore a person responsible for choosing the mitigation methods for the entity should be able to consider a number of protection/mitigation methods and their monetary values before the proposal is submitted to the management.