15. Exercise: Cost of ICT incident calculation

Main Objective	Make the CERT team familiar with one solution for estimating the costs of different information security incidents	
Targeted Audience	Managers of CERT staff, incident handlers who have to estimate losses	
Total Duration	2 hours (120 minutes)	
Time Schedule	Introduction to the exercise	15 minutes
	Task 1: Describe the working environment	15 minutes
	Task 2: Analyse the incidents	45 minutes
	Task 3: Compare the costs of the incidents	15 minutes
	Task 4: Small practical example	15 minutes
	Summary of the exercise	15 minutes
Frequency	Once per team	

15.1 GENERAL DESCRIPTION

The knowledge of the economic value and impact of the security incidents is of significant importance for the CERT teams and for the companies' management. This awareness allows the CERT managers to properly assess the cost of CERTs (including proper staffing and equipment/software investment/expenditure). Therefore, it is important that the teams understand the monetary value of their work.

When requesting the funding of a security team (or internal CERT), a manager should be able to justify the value to the company and the requested amount. This is achieved by showing how much money is at risk without the investment and how much can be saved if a security incident happens and the company is properly prepared. It is important to be able to estimate their monetary values and to select the mitigation measures that decrease the loss occurrences most effectively (largest savings compared to the smallest costs/investments).

This exercise allows the CERT team to estimate the cost of a computer security incident. The presented numbers are based on real companies and colleges and on incidents that have actually happened (information gained through authors' private sources and the literature quoted). For instance, DDoS attack costs were based on an actual incident in an Internet store incident that occurred and was analysed in 2012.

The exercise additionally introduces a calculation model and a common language to estimate and discuss the cost of incidents. It helps to realize that:

- incidents affect numerous and various activities, such as daily operations, but also legal staff, top management, etc.;

- components of losses depend on the type of victim’s activity; the exercise is performed for two very different organisations and the Exercise participants will learn that a similar incident will have a different impact on each analysed entity;
- calculation of the total incident cost is generally significantly larger than intuitively anticipated; especially, labour costs of the employees who do not work (or have to repeat their work) during and after the incidents cost the most;
- this knowledge is helpful to support a decision on the security measures to be undertaken and helps to calculate the return on security investment (ROSI).

The CERT member will work with several spreadsheets, each spreadsheet devoted to one of the five most common security incidents (Ponemon Institute, 2012). Each incident will be analysed in the case of two different entities: an Internet store and a college (the word ‘entity’ will be used as a word for both of these organisations). Each of these two types of entities has its own specifics: the Internet store has a large turnover, and each second of its inactivity generates a significant loss; a college handles a significant number of students who pay their tuition and an idle time is a loss for them.

The costs of the damages of these incidents are collected and compared in the last spreadsheets, where the expected incident frequencies are added, allowing an estimate of a yearly expected cost of incident and total cost of security incidents to be calculated. These calculations then permit a comparison with the planned budget of the security measures.

15.1.1 Terminology

Annual loss expectancy (ALE) – the expected value (cost) of a yearly occurrence of incidents of given type, in monetary units. It is a product of SLE and ARO (SLE*ARO). The ALE for each type of incident is different.

Annual rate of occurrence (ARO) – expected number of an incident’s occurrences during a calendar year. For rare incidents, it is equivalent to a probability of one or more incidents during a year; for frequent incidents, it is equivalent to the expected number of incidents per year. The ARO for each type of incidents is different.

Gross margin – the difference between revenue and cost before accounting for certain other costs. Generally, it is calculated as the total selling price of the items sold (revenue), less the cost of goods sold (production or acquisition costs).

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 VAT) of all products sold during the fiscal year.

Single loss expectancy (SLE) – the expected value (cost) of an incident in monetary units, assuming its single occurrence. The SLE for each type of incidents is different.

Total ALE (TALE) – the total expected annual loss expectancy from all types of incidents considered.

15.2 EXERCISE COURSE

The course of this exercise is as follows. All assumptions and discussions should be moderated by the trainer.

15.2.1 Introduction to the exercise

1. Explain the scenario.
2. Explain the goal.
3. Explain the tool (the workbook); ask students to open the workbook on Virtual image. To do this a student should open the catalogue: /usr/share/trainee/15_CIC/adds and open the workbook Exercise 15 Calculator – CIC or Exercise 15 Calculator – CIC Open (in Microsoft .xlsx format or in open .ods format).

15.2.2 Task 1 Describe the working environment

Ask the students to fill the first spread sheet with the assumed numbers, specific to your country. The currency used in the workbook is EUR. Consider a company and a college to be of a comparable size: about 100 employees. An Internet store of such a size must have at least EUR 100–200 million to be profitable, depending on the average achieved gross margin, salaries and overheads (company costs should be smaller than the revenue times gross margin).

The college business model is based on students' tuitions. If there are 2,000 students, then each student must pay at least around EUR 6,000 tuition per year for the college to be profitable, also depending on the staff salaries and overheads.

This amount (tuition) is important since this is also a measure of a value lost during some of incidents: while a student pays their tuition, they may not be able to participate in some activities in the course due to the lack of the computer or Internet access when needed and may have a feeling of a wasted time (= money). As a consequence, the student also loses confidence in the college, its image is impaired and the process of repairing this image is long and costly.

The initial assumed numbers are given in the table, can and should be altered by students. However, the moderator should take care that they are internally consistent (e.g. if the store's revenue or gross margin is lowered then the number of employees must be smaller for the store to stay in profit).

15.2.3 Task 2 Analyse the incidents

The incident scenarios are prepared in such a way that between two and six assumptions (the numbers on the yellow background) are necessary to make for each kind of scenarios. They can and should be altered by students in a controlled way, i.e. the student should be encouraged to alter these numbers, but their meaning should be discussed and kept in mind.

15.2.4 Incident 1: Spam

The entity is attacked by spam in a large volume. The installed filters are 99% effective (a different level of effectiveness can be chosen) (Wiehe *et al*, 2006). How much might it cost to deal with the remaining 1%? It is important to consider the time devoted by an average employee to removing unwanted mail from the mailbox. The total time can be up to several seconds per spam mail. How much does it cost the entity per year?

15.2.5 Incident 2: Virus

A virus attacks the entity and causes a loss of one day of work for 20% of the employees (and students in the college). Before they can resume their work, the IT department has to identify the problem, find a solution (taking two hours) and repair each of the affected computers (30 minutes for each). In all, 60% of IT department is involved in the identification/cleaning process.

Additionally, some systems have had to be reinstalled and additional work by the IT department is necessary. It took six days of work to reinstall the systems and solve all the outstanding issues. This time was used also to consult the students on their reinstallments.

Many students' laptops were infected while working at the college premises. They lost a significant amount of time while reinstalling their systems.

Although it took only two hours to identify the problem and find a cure, cleaning hundreds of students' laptops was an overwhelmingly large task for four IT department employees; in addition, each employee and student lost one day because their work has not been backed-up prior to the incident.

15.2.6 Incident 3: Distributed Denial of Service (DDoS) attack

The entity has been attacked by a DDoS attack. The web page became inaccessible. The attack lasted 36 hours and its starting time meant that that if affected 1.5 working days. The impact on the college was different than that on the store, since the store business is much more dependent on its web page: most losses for the store were connected with loss of orders, idle time of many employees, and disturbances in the backlog and just-in-time processing. The college's losses were connected mostly with the idle time of a few employees and some additional work load for the IT/security department. But if the college offers some distance-learning modes, the losses can be significant. It is assumed 20% of all students participate in this form of learning.

The lost labour cost is equal to the duration of the attack x the number of the employees, whose work is affected by the attack x the level of the loss of their efficiency x their salary increased by the additional personnel costs and other costs.

The lost income is the time when the web site is not operational (here we assume the sales are proceeding evenly round the clock) x the average margin.

We do not include in this calculation a loss of confidence, image impairment and their high restoration costs, although these can be tremendous: some Internet companies had to close after a cyber-attack due to their loss of image.

15.2.7 Incident 4: Data theft

It has been discovered that due to the IT system security breach a part of the database containing personal data of a large number of customers/actual and former students was stolen. To cover the damages, 1,000 people received EUR 1,000 each in compensation. This is a typical loss for a small company in the data theft case (see Verizon, 2012, tables 12 and 13).

The incident has additionally consumed a lot of time of lawyers, top managers; furthermore, significant external fees had to be paid (for external consultants and court fees).

Additionally, over the following year 5% of the Internet store's customers were lost as the stores reputation suffered (Ponemon Institute study, 2011), these customers deciding to purchase goods from another store. Similarly, for the college, 5% of new students decided to enlist in other colleges (compared with the total number of new students entering the three-year programme offered), because of lack of trust in the college, after the incident.

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

A law enforcement agency (LEA) has entered the entity's premises claiming one of the entity's computers has been sending out illegal content (e.g. child pornography). LEA officers have seized a number of the entity's computers, fortunately not affecting the main store business. However, for the proper further operation of the store (in light of the fact that the computers may remain in a custody for a long time) the entity had to immediately purchase new equipment for EUR 30,000, wait for its delivery and install the computers.

The visit caused a lot of excitement among the employees, who were discussing the case instead of working. Also, due to the LEA seizure, some of the work of IT people had to be redone. The entity also had to provide extensive documentation, which in total cost it 20 days of work. Additionally, IT department employees, lawyers and a representative of top management had to prepare documents and testify at the prosecutor's office. Additionally some staff members were interrogated by the LEA.

15.2.9 Task 3 Compare the costs of the incidents

In each of the spreadsheets there are additional positions to be considered, like costs of lost reputation and trust, and know-how. These costs should be considered in the particular cases and here are assumed to be zero (in a conservative approach).

The results are collected in the 'Comparison' spreadsheet for the Internet store and for the college. The student should remember that the results represent only five among numerous kinds of security incidents. The results (in the top row) copied from individual analyses are called single loss expectancy (SLE).

For each of the security incidents a probability that it will happen during one year is assumed. These numbers are called annual rate of occurrence (ARO). The reciprocal of the probability (frequency) is mean average time between incidents of a given type in a given entity, in years. They should be discussed and altered, if needed, based on individual experience.

Below are the products of the costs and the frequencies, equivalent to the expected yearly costs of a given incident. These figures are called annualised loss expectancy (ALE). The sum of the costs for all possible incidents for a given entity is the total expected yearly cost of the security incidents in a given entity (TALE = Total ALE).

Depending on a particular, considered investment, the expected yearly costs for a given security incident (if the investment is to mitigate only one kind of incidents) or the total security incidents costs (if the investment is planned to mitigate a number of the incidents' kinds) should be compared to the investment's yearly amortisation.

If an investment *I* is considered as reducing *ALE* by *X*% (or a number of ALE_i by X_i %) for *N* years, then *ROSI* parameter should be calculated as $ROSI = (N * \sum(ALE_i * X_i) - I) / I$. If *ROSI* is positive then this investment should be accepted.

15.2.10 Short practical case

To decrease expected losses, purchase of a new security appliance is considered. It is an IDS/IPS and the testing has shown that probably it will further decrease virus penetration occurrence and the botnet annual rate of occurrence by two times. It will not provide any additional shield against spam, DDoS or data theft. The appliance costs EUR 15,000. The above effectiveness will be maintained for three years and therefore the appliance's amortisation is assumed to be three years.

Should the Internet store or the college purchase this appliance and what will be the cost-efficiency rate?

Solution
N years times the sum of ALEs multiplied by their effectiveness's (50% for virus and botnet and 0 for the other possible security incidents) is smaller than the appliance's purchase price for the Internet store and higher for the college. Therefore the expenditure of EUR 15,000 is justified for the college, while the store should instead look for more efficient tools to mitigate DDoS and data theft threats. Students are encouraged to repeat the calculation with a different mitigation application, consider the results and discuss the differences.

15.3 Summary of the exercise

Some points for use for wrap-up and conclusions in the summary:

- The cost of the security incident depends greatly on the kind of incident, the type of affected entity and its scale. The incidents that involve legal consequences may be the most expensive ones.
- Expected ALE depends heavily on the expected probability of incident occurrence, ARO. ARO depends on the type of incident and the kind of entity attacked. There are different

rationales to attack an Internet store (mostly economic, to generate losses for such a company) and a college, therefore the expected frequencies of their occurrences are also different.

- This analysis helps to compare the ALE and Total ALE of the security breaches with the considered investments of the equipment reducing the risks.
- The calculated costs can be compared with the typical incident costs published in the literature (Ponemon Institute, 2012, Figure 9): obtained costs are smaller due to the small entity sizes considered.
- There is a strong knowledge base needed to support a funding demand for new security measures. Decision makers need this analysis.
- What if the technical mitigation is not beneficial? Should we always accept the risk? Introduce the possibility to insure the assets in that case.

15.4 REFERENCES AND FURTHER READING

1. Anderson, Ross, et al., *Measuring the Cost of Cybercrime*, 2012 (http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf)
2. Information Security & Business Continuity Academy, Free Return on Security Investment Calculator, 2012 (http://www.iso27001standard.com/en/rosi/return-on-security-investment#)
3. Lepofsky, Ron, *Quantifying Risk and Cost of IT Security Compliance*, ERE – Information Security Auditors, 2010 (http://www.ere-security.ca/PDF/html/Quantifying%20Risk%20and%20Cost%20of%20IT%20Security%20Compliance.html)
4. Ponemon Institute, *Reputation Impact of a Data Breach – Executive Summary*, 2011, (http://media.scmagazineus.com/documents/30/ponemon_reputation_impact_of_a_7405.pdf)
5. Ponemon Institite, *The Impact of Cybercrime on Business*, 2012 (http://www.checkpoint.com/products/downloads/whitepapers/ponemon-cybercrime-2012.pdf)
6. Verizon 2012 Data Breach Investigation Report, 2012 (http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

Wiehe, Anders; Hjelmås, Erik; and Wolthusen, Stephen D. , *Quantitative Analysis of Efficient Antispam Techniques*, Proceedings of the 2006 IEEE, Workshop on Information Assurance, United States Military Academy, West Point, NY, 2006 (http://www.docstoc.com/docs/69747732/Quantitative-Analysis-of-Efficient-Antispam-Techniquespdf)