

Exam Security in Organizations

Date: January 18, 2010

Time: 10.30 – 12.30

This exam consists of three parts (A, B and C). Part A is multiple choice (25 questions) and parts B and C are open questions (10 and 5 questions, respectively). For each multiple choice question in part A you can score 1 points; for each of the open questions in part B and C 3 point for a (maximal) total of 70 points. Your final grade for the exam will be $1 + 9 * (\text{Total Points} / 70)$.

A. Multiple Choice (25 questions)

For each of the questions below, please choose precisely one answer namely the best possible answer. For each question one can earn 1 point.

Question #A.1

What is the most important objective of information security for an organization?

- a) Preventing hackers breaking in the computer systems of the organization.
- b) Preventing the outbreak of viruses and worms within the organization.
- c) Implementing all the 133 controls described in the ISO 27002 standard.
- d) Management of the organization being in control of the risks related to confidentiality, integrity and availability of information.

Question #A.2

An example of treating a risk by transferring it, is:

- a) Using a ISO 27001 certified courier service for shipment of backup tapes.
- b) Using IPSEC to encrypt network traffic.
- c) Taking an insurance policy
- d) To accept a risk.

Question #A.3

A message presented to users telling them when they logged on the last time is an example of a:

- a) Preventive control
- b) Detective control
- c) Corrective control
- d) Repressive control

Question #A.4

The importance of security incident management lies in:

- a) Being able to quickly respond to attacks, limiting the damage and simplifying correcting the damage caused by the incident.
- b) Being able to learn from violations that happened in the past
- c) Providing input to risk assessments
- d) All of the above.

Question #A.5

End responsible for information security within an organization is/are:

- a) The Employees of the organization

- b) The IT manager
- c) The management of the organization
- d) All of the above.

Question #A.6

An organization implements ISO 27002 control 8.1.2 'Screening' by requiring new employees to hand in a VOG statement ('Verklaring omtrent gedrag', or police clearance certificate in English) before their first working day. What is a typical fundamental shortcoming in this implementation:

- a) Employees forget to hand in their VOG statement.
- b) The VOG statement is not checked by the organization.
- c) Prospect employees are already told confidential information during the job interviews.
- d) Personnel of suppliers do not fall under this control.

Question #A.7

Input for an information security management system (ISMS) are:

- a) Obligations set by law
- b) The risk perception of an organization
- c) Contractual obligations
- d) All of the above.

Question #A.8

What was the reason the British Standard 7799 part 1 (the predecessor of ISO 27002) was supplemented with a part 2 (the predecessor of ISO 27001)?

- a) Information security is a process.
- b) This was necessary to become an ISO standard.
- c) BS 7799 part 1 was too limited on user management, anti-virus control and fishing attacks.
- d) BS 7799 part 1 was not suitable for the USA as it was based on British law.

Question #A.9

What is the benefit for a Dutch organization to become certified against ISO 27001?

- a) It is necessary in order to become really secure
- b) It is required by the ISO 27006 standard
- c) It is required by Dutch law
- d) It is a convenient way to provide evidence to external parties that the organization is in control of information security

Question #A.10

What would be a possible vulnerability in the usage of an answering machine?

- a) Spoofing
- b) Unprotected remote access
- c) Buffer overflow
- d) No vulnerabilities exist as answering machines are not considered IT systems

Question #A.11

Why is it important that i) each business information system has an 'owner' and ii) that this owner is a business manager and not the IT manager.

- a) Without an owner nobody feels responsible and if the IT manager is the owner he will make the system too secure.
- b) Without an owner nobody is accountable and the IT manager is typically not aware of the business risks related to the information system.
- c) Without an owner nobody will pay for information security of the system and the IT manager is typically not aware of the business risks related to the information system.
- d) Without an owner the information system will not be properly used and the IT manager does not really care about security.

Question #A.12

Which of the following do represent input to Business Continuity Management (BCM):

- a) Swine Flu (known in the Netherlands as the Mexican Flu)
- b) Fire, flooding, lightning, loss of power
- c) Computer viruses
- d) All of the above

Question #A.13

Suppose there are two persons with exactly the same first and last names, say Ronald John Doe. How, in the context of digital certificates (X.509), can a relying party distinguish the two persons solely based on the issued, qualified certificates?

- a) Qualified certificates always contain a birth date and birth place.
- b) They can be distinguished by the serial number.
- c) They can be distinguished by the Distinguished Name.
- d) They typically cannot be distinguished.

Question #A.14

In the context of qualified certificates (X.509), why would a Certificate Service Provider (CSP) be obliged to keep copies of identity documents of the persons they have issued certificates for?

- a) As evidence in case the persons do not pay their invoices.
- b) In case of disputes.
- c) For re-issuance of certificates.
- d) It is an explicit requirement from the European Directive on Electronic Signatures.

Question #A.15

Why does the European Directive on Electronic Signatures speak of electronic signature instead of digital signatures which is common in cryptography?

- a) The term 'digital signature' originates from the US and the European Commission wants to avoid confusion.
- b) Cryptographers have all kinds of 'digital signatures' implying that the term 'digital signature' is broader than what is meant with an 'electronic signature'.
- c) What is meant with an 'electronic signature' in the directive is broader than what is meant with 'digital signature' in cryptography.
- d) There is no reason.

Question #A.16

What is the first thing an organization needs to consider before collecting personal data in an internet web based application?

- a) Information security
- b) Using SSL
- c) Using secure cookies
- d) Analyze if the organization has a legal basis to do so

Question #A.17

In the customer database of an internet web based application an organization has removed all client name and address information of its clients but not their IP addresses (issued by their ISPs). Can the organization justly claim this database is anonymized?

- a) Yes, IP addresses are anonymous
- b) Yes, IP addresses are too dynamic to link persons too (DHCP)
- c) No, IP addresses are directly linked to persons.
- d) No, IP addresses are indirectly linked to persons.

Question #A.18

An IT auditor has reviewed a document that outlines the information security of an organization and writes a report on it. What would be the 'assurance level' in the report?

- a) Design
- b) Existence
- c) Operational Effectiveness
- d) Depends on the auditor

Question #A.19

A company is outsourcing its IT to an external party. As information security is considered important by the company it is required that the external party is certified against ISO 27001. Would the fact that an external party is ISO 27001 certified be sufficient for the company to be in control of its information security?

- a) Yes, that is what the ISO 27001 certification is meant for.
- b) No, the external party needs to be compliant with ISO 27002 not with ISO 27001.
- c) Yes, as ISO 27002 is normatively referred to by ISO 27001.
- d) No, the company needs to further specify its security requirements to the external company.

Question #A.20

A company is bringing a new mass consumer product into the market, due to the innovative character of the product the actual sale numbers of the product are considered commercially sensitive by the company. To stimulate sales the company has placed a unique code on each product consisting of 11 digits. With this code the consumer can win a price; the consumer needs to enter this code at the company website to see if the consumer has won the price or not. The code is developed by the IT department of the company itself and effectively is an encryption of a serial number that starts at 1 (with product number 1) and so on.

What would be the security objectives of the encryption in the codes?

- a) Authenticity
- b) Non-repudiation
- c) Confidentiality
- d) Authenticity and Confidentiality

Question #A.21

An organization is implementing the ISO 27001 standard. Within the organization ten business units exist. In each of these units many different complex IT related processes exist. Typically these processes are different to understand for people outside the business units. As one of the first steps, the organization has appointed a security officer. The security officer has created a risk assessment and treatment methodology from the ISO 27005 standard and has used this to identify the high risks in the business units. To this end, he has organized workshops where knowledgeable employees participated that work in the business units but do not have management responsibilities.

The workshops were very successful in the sense that many high risks have been identified and many additional security controls have been suggested. Some risks were accepted during the workshop. As a finalization of each of the risk assessments the security officer has formally approved the results of the workshops and the next stage of the ISO 27001 implementation project is to implement the identified additional security controls. What is wrong in this setup?

- a) The security officer should not approve the results of the risk assessments but the management of the business units.
- b) The ISO 27005 does not deal with risk assessments but with the requirements on certification bodies.
- c) The security officer should not create a risk assessment and treatment methodology as this results in a conflict of interest.
- d) Employees from the business units should not participate in the workshops as they typically know nothing about information security.

Question #A.22

Cross Site Scripting (XSS) is the most exploited vulnerability in web applications (OWASP Top 10, 2007). What is the main vulnerability that allows this kind of attacks?

- a) The webserver is not patched with the latest software updates.
- b) The user input of the website is not properly sanitized and used directly in the output again.
- c) The forms on a website can be adapted such that different data is sent to the server.
- d) The users are unaware of the danger and visit evil and honest websites simultaneously.

Question #A.23

A less heard of but very powerful attack is Cross Site Request Forgery (XSRF). Which control will help to some extent to prevent XSRF attacks from the perspective of the website?

- a) Label every form in a web application with a random number. The server remembers the provided numbers for a specific session. Only the submitted forms containing this number are considered valid requests and can only be used one time.
- b) Use the latest version of a browser and disable the flash plugin.
- c) Make use of CAPTCHA's (Completely Automated Public Turing-test to tell Computers and Humans Apart) for every request that has big consequences.
- d) Make sure that people never click on any untrusted link or object on a website.

Question #A.24

A user wants to start using web based electronic banking. Which of the suggestions below would be the best control against XSRF from the perspective of the user?

- a) Use an Apple computer as these are not susceptible to XSRF attacks.
- b) Use one browser type only for electronic banking (e.g. Opera) and another type of browser for other internet applications.
- c) Disable Javascript.
- d) Always inspect the HTTPS certificate that forms the electronic banking secure connection.

Question #A.25

Your consulting firm has won a contract for a small technology firm. Your CEO has decided that its proprietary technology is worth protecting. Which of the following is *not* a reason why this firm should develop an information classification?

- a) Information classification should be implemented to demonstrate the organization's commitment to good security practices.
- b) Information classification should be implemented to ensure successful prosecution of intellectual property violators.
- c) Information classification identifies which level of protection should be applied to the organization's data.
- d) Information classification should be implemented to meet regulatory and industry standards.

B. SCADA Security (10 questions)

Answer the questions in a brief manner. Base your answer on the information in the introduction below unless stated differently by usage of the words 'imagine' or 'think'. For each question one can earn at most 3 points.

Introduction

SCADA is an acronym that stands for Supervisory Control and Data Acquisition. SCADA refers to an information system that allows control of industrial processes. Prominent examples are the chemical industry (petrochemical, food industry), power plants (electricity, nuclear, gas) and public utilities (drinking water, sewerage systems, sluice control).

A SCADA system performs two tasks: it collects data from the processes under its control through sensors (e.g., thermometers, pressure meters, voltage meters) and it regulates the processes by sending instructions ('set points') to appliances (e.g., mechanical valves, heaters). As an example in the chemical industry: a SCADA system monitoring a chemical process might notice through a connected thermometer that the reaction vessel is not hot enough and it then sends an instruction to a gas valve of a heater to open up a bit further, heating up the reaction vessel.

Roughly speaking a SCADA system consists of three layers nowadays all connected through computer networks:

Man Machine Interface (MMI)

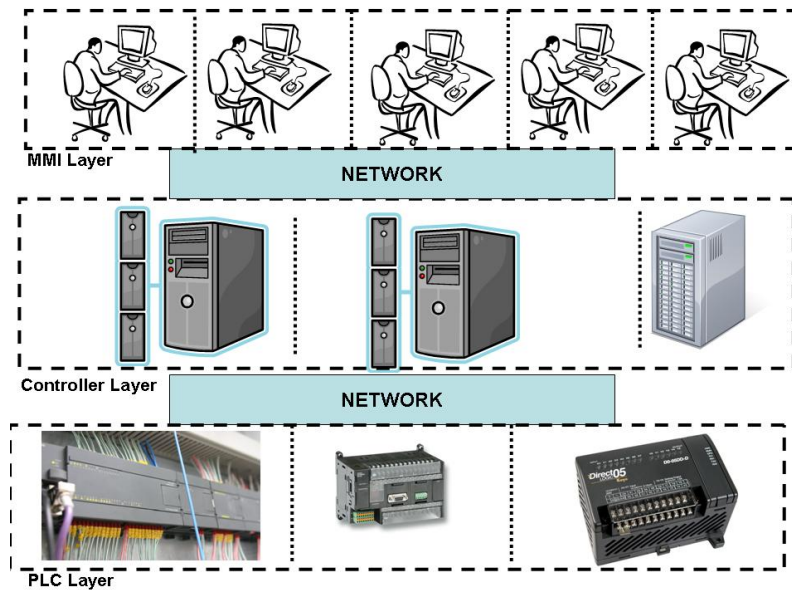
- These are workstations running specific user applications used by 'process operators' located in control rooms. They monitor the processes and can intervene if necessary. The workstations used, resemble those used in an office automation context; the difference lies in the SCADA applications run on the workstations.

Controller layer

- These are servers running specific applications connecting the MMIs with the Operational Layer: instructions sent by the MMI are translated by the server application to specific hardware instructions and sent down to the Operational layer. This layer also contains business logic: it 'knows' that if something is below or above a certain threshold, it should intervene or alarm a process operator. The servers used resemble those in an office automation context; the difference lies in the server applications run.

Operational Layer (or PLC layer)

- This layer contains the 'actuals' that actually control the process, e.g. the thermometers and the valves. Network access to these is done through so-called Programmable Logic Controllers (PLCs) that are equipped with an Ethernet port. PLCs connect to the 'actuals' by (serial cables) or so-called field busses; for the purpose of this exam these connections are not relevant. PLCs have no analogue in the office automation context. Typically they are placed in an industrial context, implying that they need to comply with certain safety and robustness requirements, e.g., they will not produce sparks in order not to set fire.



SCADA systems have evolved over time in various steps:

- a) Originally they were pure mechanical devices that were manually operated by pushing/pulling valves; sensors had to be read by the process operators by looking at them.
- b) Then it was convenient to have these valves operated mechanically and to have them controlled by a simple computer and to have the sensor readings depicted on the computer screen.
- c) The simple computer then evolved from being close to the device using a LAN to a server based solution using a WAN. The Controller and MMI Layers evolved to being centrally organized; typically far away from the Operational Layers they control. Actually the various components in each of the three layers are typically scattered over different locations themselves, creating one big distributed system.
- d) The usage of closed, ‘proprietary’ systems and (network) protocols have been replaced by standard systems like Windows and Linux and open standards like TCP/IP and Ethernet. The SCADA industry has also developed an open message specification (Manufacturing Messaging Specification or MMS) enabling open communication between the controller and the operational layer. This enables the integration of SCADA systems of various manufacturers.
- e) SCADA systems used to be islands not connected to the corporate office network, but this is changing too. SCADA systems get more and more connected to the corporate office network to provide business information.
- f) The current development is to further automate the process control itself, requiring human operators only to intervene if everything fails implying a further reduction of operator staff.

In this evolution information security has not always been taken into account properly. To indicate, network authentication between the various layers is typically not implemented. SCADA systems are typically real-time systems implying that performance and availability are the most important aspects. Due to this, manufacturers are sometimes reluctant to supplement their installations with security patches of (network) operating systems and standard IT technology, e.g. databases and web servers, as this could harm availability (‘if it is not broke, don’t fix it’). Typically centralized SCADA systems can fall back to local mode: locations that are typically centrally controlled using a WAN still contain local control rooms

with workstations enabling local control in case the WAN fails or the central control room breaks down.

Questions

Question #B.1

Based on the introduction, describe two prominent vulnerabilities in SCADA infrastructures in at most 5 sentences.

Question #B.2

In the context of a SCADA system used in the power infrastructure, imagine a prominent example of a malicious human threat targeting the availability. Answer in at most one sentence.

Question #B.3

Imagine what information inside SCADA systems in the chemical industry would be confidential? Hint: think of Coca Cola. In the context of a SCADA system used in the chemical industry, imagine a prominent example of a malicious human threat targeting the confidentiality.

Question #B.4

In at most 3 sentences imagine an example of a SCADA context where the integrity (correctness) of what kind of information inside SCADA systems is vital. Think of an example of a malicious threat targeting this integrity.

Question #B.5

Typically a SCADA power infrastructure comprises of many small locations (e.g. transformer houses) scattered over the country. Suppose that the power infrastructure uses one, transparently routed network for SCADA communications, sketch a scenario combining one vulnerability from Question #B.1 with the threat you answered in Question #B.2.

Question #B.6

In an office automation context, the workstations are often configured with 'automatic screen locks'. That is, after a certain amount of time (e.g., 10 minutes) the workstation is 'locked' and the user needs to type in his password to access it again. In at most 2 sentences give an example of a threat that is addressed with this control. In the context of time critical SCADA systems the MMI workstations of process controllers are usually not equipped with automatic screen locks. Why do think this is the case?

Question #B.7

Do you think that the threats related with 'automatic screen locks' are not relevant in the SCADA context, or if think they are, how would you think they are alternatively addressed in that context?

Question #B.8

Describe in at most 5 sentences, how you would address the concern SCADA manufacturers have in supplementing security patches to their installations?

Question #B.9

Suppose one is writing a Business Continuity Plan (BCP) for a typical SCADA infrastructure scattered over the country that is managed from a central control room using a WAN. In at most 5 sentences describe two prominent scenarios that need to be addressed in the BCP. Base your answer on the information in the introduction!

Question #B.10

Describe in at most 5 sentences the most important working alternative the BCP will be based on. Base your answer on the information in the introduction!

C. CardSystems Solutions Inc. (5 questions)

Answer the questions in a brief manner. For each question one can earn at most 3 points.

A security breach at CardSystem Solutions Inc. in Arizona in 2005 has exposed 40 million credit card customers to possible fraud. It is considered one of the largest card-information heists ever.

CardSystem is a third-party processing facility, which performs back office processing for creditcard companies such as MasterCard and Visa. It performs payment processing, but there is absolutely no functional or technical need to store these transactions for future use.

Hackers took advantage of a network vulnerability (a misconfigured firewall) and installed a program on CardSystem's servers that allowed them to download customer information. It is unclear how long the information was being viewed or downloaded.

The incident calls into question both the sloppy handling of customers' personal information as well as lapses in security measures.

Interestingly enough, only three months before this security breach, CardSystem's security had been certified by the auditing company Savvis Inc. against a security standard (the Cardholder Information Security Program standard) authored by various credit card companies. Proper auditing would have detected such problems in its earliest stages, but the security breach was apparently detected by MasterCard after they noticed fraudulent activity on their customer accounts.

(Source: Seattle Times, June 25th 2005; Yahoo News, June 29th 2005).

Question #C.1

Based on the information above, describe in one sentence a fundamental flaw present in the data storage of the systems at CardSystems.

Question #C.2

Had this incident occurred in The Netherlands (or anywhere within the European Union) CardSystems would very likely violate privacy regulations. Give in at most 5 sentences an argument why this is so.

Question #C.3

Apparently not only did the security at CardSystem Solutions Inc. fail, but also the auditor Savvis Inc. failed. One point to come forward in a (civil) court case was that even if Savvis verified proper configuration of the firewall (three months prior to the security breach), misconfiguration could have occurred afterwards. What control could have been installed to minimize the possibility of the happening?

Question #C.4

Continuing from #C.3, what should Savvis have checked to be able to certify, with appropriate confidence, that the firewall would always be properly configured?

Question #C.5

Describe in at most 5 sentences a technical control that could have prevented a program being installed that accessed customer files.