Security in Organizations: Assignment 5

Group number 27

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

As specified by Ms. Guinet, we want to specify that we could not adhere to the 4 page limit but we kept it under 5 pages.

A

a.
- Prevent leakage of sensitive information to other people in the same house.
- Keep a lock on sensitive equipment and documents (e.g. for when a burglary happens).
- Logging work hours.
- Using online communication tools for all communication with colleagues and external parties.

b. There is now a lot of overhead for normal employees with all the new responsibilities that they now have. Philips is a company that spends a significant amount of money (around 10% of annual revenue) on R&D and would like to keep this information secret, so people that work from home have to follow strict new guidelines to keep this information secret.

In addition to that, the employees now have less contact with their colleagues, which can negatively impact them mentally.

B

a.
- Remote access applications (SSH, Windows Remote Desktop, Citrix, etc...).
- Virtual Private Network (for remote access to internal network).
- Applications like Teamviewer (to grant control of your PC in case of help needed).
- Application that keeps track of working hours.

- Online communication tools if this was not the case before.
- Video conferencing software (e.g. Zoom, Microsoft Teams).

b. There are now more applications that they have to get used to and have installed, in addition to having to follow an entire new procedure to being capable of working. All these new applications makes it more difficult for an employee to follow the security policy of the company.

C

Let ’Group2’ be the group of Philips employees who develop embedded software used in Philips products. This group needs to take some unreleased products home to test their software.

D

Group1:

(a) A Physical attacker can steal the personal information of the employees. This is bad because the company is supposed to protect the personal information of it’s employees by law.

(b) Someone that visits or lives at the home the employee is working from can see information about employees they are not allowed to see. Phillips would not want some random person to know about who is earning how much and other information about employees.

(c) A disgruntled employee can change their own (or someone else’s) salary if they are visiting, legally or illegally, the HR coworker. This loses the company money or causes chaos for the administration, so this is obviously terrible.

Group2:

(a) A physical attacker can steal unreleased Philips product that are still in development, possibly leaking sensitive information about their products. This information can be used by competitors which could negatively impact the sales of Philips products.

(b) The embedded development processes of Philips products can be leaked to other people in the same house (or through a window), which could also be used by competitors.

(c) The source code or other sensitive details about the embedded software can be stolen by a physical attacker, which can then be used by hackers to break into the products of Philips.

E

These vulnerabilities apply to both groups:

1. The device that is being worked on can be compromised by malware caused by personal use or a vulnerability in one of the applications that is being used for teleworking.

2. A device in the same network was infected and spread to the device that is being worked on (e.g. because the device was not updated with a security patch).

Group1: These vulnerabilities could leak company information and more specifically information on employees, like their addresses and their BSN.

Group2: These vulnerabilities could cause malware to spreak further into the internal networks of Philips. It could also leak sensitive product information, embedded software or development processes to competitors. A hacker could also secretly alter the code to make Philips products vulnerable or to make them break earlier.

F

Group1:

1: A burglar breaks into the house, breaks into the working device and steals the personal information of the employees. The burglar then can commit identify fraud with the information they received from that break-in and commit a lot of heinous crimes and ruin a lot of lives. *(D.a)*

2: The child of an HR employee sees personal information of an employee and decide to use it to their advantage. *(D.b)*

3: A colleague can come over and while the HR employee is grabbing some tea/coffee or is taking a quick bathroom visit, the disgruntled employee changes they salary of that annoying colleague that keeps pestering them. *(D.c)*

4: The employee wanted to watch the new Spider-Man movie but did not want to pay so they illegally downloaded it and accidentally got a virus on the same device they use for work. Now the device is compromised and they will be broadcasting all sensitive data to the creator of the malware. *(E.1)*

5: The employee has not updated their work device and is thus vulnerable to an home network attack in which the attacker has infected another user on the network, and then uses a vulnerability to attack the device the employee is working on. The hacker can then sell all personal information found on the device. *(E.2)*

Group2:

1: A burglar that is hired by a competitor steals a product of Philips in the house of an employee that is still in development. *(D.a)*

2: A competitor makes a deal with a housemate of the employee to send them information of the development processes. *(D.b)*

3: A physical hacker is hired by a competitor to secretly break into the house of an employee and copy the code and all other information about the products the employee is working on. *(D.c)*

4: A terrorist organisation targets an employee working on medical devices (e.g. respiratory equipment) using a vulnerability found in one of the applications the employee uses (for personal use or teleworking), and secretly add hidden vulnerabilities to the code used in these devices which they can later use to execute an attack. *(E.1)*

5: Ransomware got into the network of an employee (e.g. via devices of other housemates), which then spreads to the internal network of Philips causing multiple business/development processes to be shut down until Philips pays the ransom. *(E.2)*

G

Group 1

a. 1: High

2: Low

3: Low

4: High

5: Medium

b. 1: A burglary is not uncommon and the impact of the personal data being stolen is potentially very high for the impacted employees.

2: This happens very rarely, as a child will not do this often, the impact is medium at it's highest, assuming the child is not an evil genius.

3: Again, this is a very rare occurrence and anything that has happened can be undone quite easily, so the impact is also very low.

4: This has a pretty high likelihood of occurring, as people tend to want to watch things for free and the impact is very high as well.

5: The likelihood is pretty low, as it's quite uncommon for someone's work device to be vulnerable, but the impact would be very high.

c. 1: Protecting sensitive information, on paper or by physically securing a laptop/desktop, while working from home is essential.

2: Making sure that no person in the house can see work-related information should be adhered to at all times.

3: Adhere to the same inter-company sharing as you would do at work.

4: Keep your working device as clean as possible and only use it for work.

5: The company should have a policy so that all the devices are updated remotely when a security update has been released.

Group 2

a. 1: Medium

2: Low

3: Low

4: Medium

5: High

b. 1: A targeted burglary is a low-medium likelihood, but the impact is medium-high if a product that is still in development gets into the hands of a competitor, because they can use it to improve their products which affects to sales of Philips.

2: The likelihood is very low, but the impact is medium because it can also help the competitors of Philips.

3: The likelihood of a burglar being hired by a competitor that is also capable of copying relevant data is very low, but the impact is medium-high.

4: The likelihood of a terrorist organisation targeting a specific employee working on medical devices is very low, but the impact would be disastrous.

5: The likelihood of that the network of an employee gets infected is medium, but the impact of ransomware is high.

c. 1: The process of physically securing confidential assets (at home) is essential, so it can less likely be stolen by a burglar.

2: It is important that employees get security awareness training so that they won't leak confidential information to others.

3: Here the process of encrypting the devices that are given to the employees is important, so that information on these devices cannot be copied without logging in.

4: The supporting process of informing employees to keep their applications up-to-date is important, but also code review and the management of rights who can commit/approve code.

5: Here it is important that the access management is done correctly so that employees (and thus their infected devices) won't have access to systems within internal networks that they don't need.

H

All the controls are from the ISO 27002:2013

Group1: 1: 11.1.2 Physical entry controls. To keep a burglar out, if this is applied then the risk is pretty much fully mitigated.

2: 11.1.5 Working in secure areas. The employee should ensure that others cannot enter their work area, which mitigates the risk.

3: 11.1.5 Working in secure areas. The employee should ensure that others cannot enter their work area, which mitigates the risk.

4: 12.2.1 Controls against malware. This is the only control against malware, this compensates only partially.

5: 12.2.1 Controls against malware. This is the only control against malware, this compensates only partially.

Group2: 1: 11.1.2 Physical entry controls. To keep a burglar out, if this is applied then the risk is pretty much fully mitigated.

2: 11.1.5 Working in secure areas. The employee should ensure that others cannot enter their work area, which mitigates the risk.

3: 11.1.2 Physical entry controls. To keep a physical hacker out, if this is applied then the risk is pretty much fully mitigated.

4: 12.6.1 Management of technical vulnerabilities. All applications used by the employee need to be kept updated and vulnerability free, this compensates for the majority, but not completely as vulnerabilities can still creep into the applications.

5: 12.2.1 Controls against malware. This is the only control against malware, this compensates only partially.