CS-E4350: Security Engineering, Spring 2021

Assignment 2

Security Risk Assessment and Investigating Human Factor Influence on Security

Introduction:

Security risk assessment is the process of identifying, analyzing and evaluating risk. It helps to ensure that the security controls you choose are appropriate to the risks your organization faces.

In order to gain an understanding of the risk assessment importance in security, read section **3.2.5 Heuristics, biases and behavioral economics** (Anderson, 2020). Please find a copy of the book by following the link:

http://libproxy.aalto.fi/login?url=https://ebookcentral.proquest.com/lib/aalto-ebooks/detail.action?docID=6412239

The following are the steps required to perform any Risk Assessment:

1. Identify the Assets
2. Identify the Threats
3. Rate the Threats using a Likelihood-Impact Matrix (See Figure below)
4. Risk Identification
5. Countermeasures

Impact

Likelihood	Trivial	Minor	Moderate	Major	Extreme
Rare	Low	Low	Low	Medium	Medium
Unlikely	Low	Low	Medium	Medium	Medium
Moderate	Low	Medium	Medium	Medium	High
Likely	Medium	Medium	Medium	High	High
Very Likely	Medium	Medium	High	High	High

Please see the ENISA report provided for a detailed explanation about performing a Risk Assessment on a Smart Car. **This example** should help you write your own Risk Assessment report on the **A Social Engineering Case Study: Manhattan Tech** **provided at the end of this document**.

In this assignment, we will also be looking at the human element in information security and privacy. After finishing this assignment, you should be able to understand and think of ways to minimize the security risks associated with human activities. The importance arises since many systems are advertised as being secure when the hardware is perhaps

that way whilst ignoring human components, thus neglecting usability issues is one of the largest causes of security and privacy failures.

To gain a deeper understanding of the role of human components in security and privacy have a look at section **8.6.8 Organizations and human behavior.** Please use the same link that is included above of the book.

For this assignment, a case study is provided that involves human elements in the security attack. You will need to perform a risk assessment on this case. If you would like to gain more understanding of the Likelihood matrix, please visit the following link: https://www.pivotpointsecurity.com/blog/using-matrix-models-for-risk-assessment/

Instructions for the Risk Assessment report:

Your report should be detailed and well thought of. You should be able to illustrate your ability to perform a detailed risk assessment on a real-life situation. The aim of this assignment is to understand the importance of the human element in the security and privacy.

General formatting instructions:

1. Font size: 12 pt.
2. Spacing: Single Spacing

This assignment consists of the following parts:

1. Read Sections **3.2.5** and **8.6.8** of Security Engineering: A Guide to Building Dependable Distributed Systems, 2020.
2. Carefully read the case study (A Social Engineering Case Study: Manhattan Tech) provided.
3. Perform the risk assessment (as detailed as possible) and utilize the likelihood-Impact matrix on the case study. You need to include **all** of the following subsections (*hint: when listing the assets think of companies from a broader context i.e., what are all the assets that companies have? apply the same broad thinking to the threats as well*):
    a. Identify the Assets
    b. Identify the Threats
    c. Rate the Threats using a Likelihood-Impact Matrix (See Figure below)
    d. Risk Identification
    e. Countermeasures
4. Answer the following questions:

    a) Include your feedback about what you have assessed. Do you think it was useful? How would you improve your assessment? Compare between the Likelihood-Impact matrix and the DREAD model (illustrate how you would rate the threats using a DREAD model). Which is more suited for this case in your opinion?

(More information on the DREAD model for qualitative risk analysis: https://resources.infosecinstitute.com/topic/qualitative-risk-analysis-dread-model/)

b) Regarding the case study, do you think the attack could have been avoided. What are some methods of awareness that you propose to protect the human elements from possible attacks? (I.e., the sender's email does not match the official email of the company). What would you like to comment on regarding the case?

c) In your opinion, do you think the CEO was correct when he refused to comment on the incident? Do you think companies should report back to clients when data breaches occur? If you were in the place of the CEO, would you have said?

Notice: This assignment is individual work and will be checked by the Turnitin system. Cheating will be addressed with following Aalto rules. Cases will be reported to the appropriate Aalto officer.

==========

Case Study

Please read this case carefully so that you can answer the questions of the second assignment.

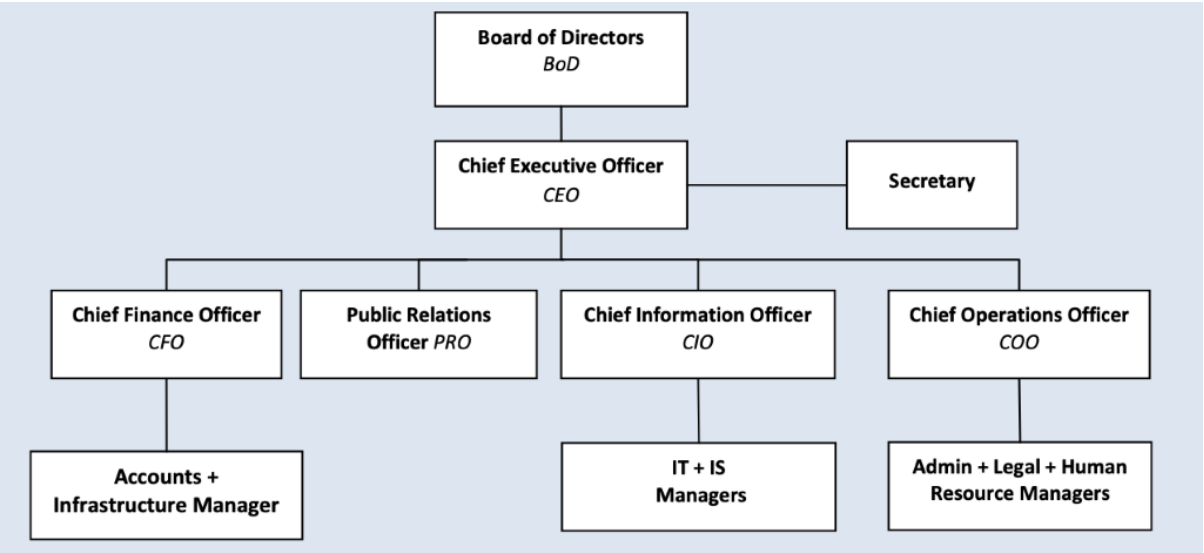
A Social Engineering Case Study: Manhattan Tech

Manhattan Tech is an agency that has become a victim to a cyber-crime attack on 18th of January 2021. The agency contacted you to produce a risk management report as part of the crisis management plan of the agency. You have offered to help in forensic investigation as well as in the recovery process of the systems. However, for the purpose of this assignment, you will only need to produce the risk assessment report.

Manhattan Tech is an organisation contracted by the Finance Authority of one of the Sub-Sahara African local governments to collect revenue in the form of taxes. The organisation uses taxpayers' information with integrity to meet local government revenue obligations such that it focuses on the developmental interests of the local government. Manhattan Tech deploys a Revenue Management System (RMS) for all taxpayers account information and revenue management. The RMS is a one-stop platform where all data is integrated and analysed. It is also integrated online to other third-party systems and tools of partner agencies and institutions such as ports clearance systems, standards clearance system among others for coordinated day-to-day operations. In addition, Manhattan Tech has contracted three other companies (Lamogi+, A&A and PAK) to provide other services of identifying new taxable businesses, maintaining and monitoring transit cargo real-time. The agency has also contracted a third-party company MyCloud to provide additional cloud services as a backup to their data centre.

The agency employs 1550 staff, 100 of which belong to the Information Technology (IT) and Information Security (IS) department. Among them are 10% of the staff is responsible for Information Security Management (ISM) in the agency while the rest with various levels of undocumented security clearances are charged with other IT support services within the company. More than half of Manhattan Tech's staff are on outsourced contract basis or internship and are on a minimum wage payment plan, which has continuously been an issue of complaint among many staffs who feel it is unfair. The figure below shows the company's management organisational structure. All the activities coordination at Manhattan Tech are dependent on the support staff at their respective workstations exchanging communications by email, phone calls or SMS alerts over the public network infrastructure for incidents management and control.

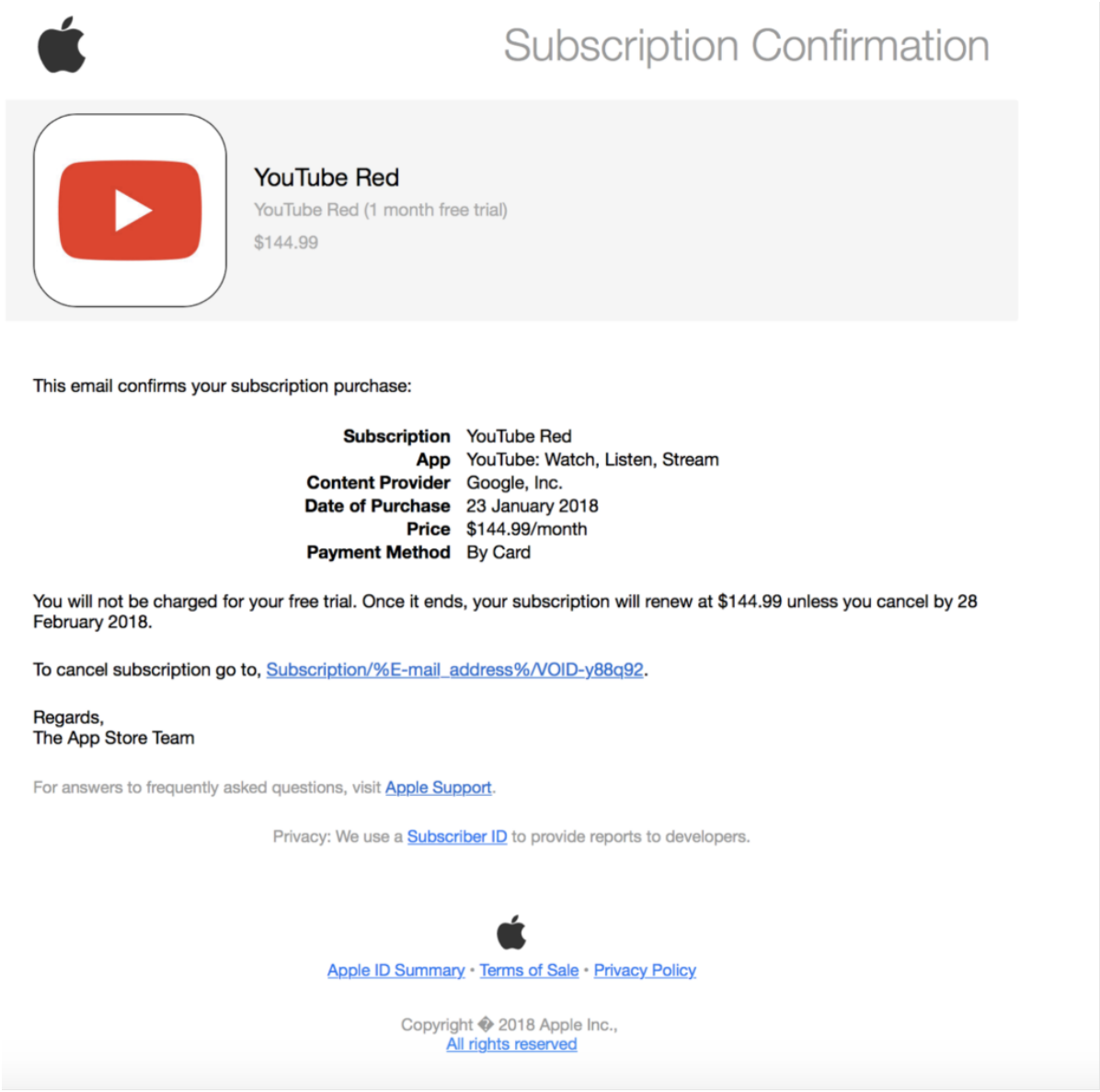
The company has had one general-purpose information security management policy for the last 10 years, but only department managers and selected staff members have been adequately trained on the policy. Implementation of the policy across the company has never been of paramount significance. However, since December 2019, the agency has had three major security breaches among other minor attempts leading to some undisclosed financial losses to the company. It is on this background that Manhattan Tech has been tasked to develop a clear and thorough Risk Management strategy and report to be presented to the stakeholders.



On the 18th of January 2021, employees discovered problems with the mail server. Shortly after that, the network turned out to be infected with Clop ransomware. Typically, a Clop ransomware blocks access to files and programs on a computer or a network. The attackers managed to block the access to systems containing financial information, email systems, the intranet, client information and backups. The company finally ended up paying the ransom of €250 K to the attackers who managed to block the access to the company's digital systems.

The Chief Executive officer refused to comment on this event to the reporters.

After forensic investigations, a report was produced to explain the cause of the event. The report stated that the Secretary received an email on the same day containing a confirmation email from YouTube regarding her subscription plan. The victim attempted to cancel her subscription by pressing the *cancel subscription link* in the email as shown in the figure below. The attackers managed to contain access to the victim's device and in turn other devices connected to the same network. The secretary explained: "The email looked a lot like it came directly from YouTube! It has got the YouTube logo and it looked official".



Subscription Confirmation

YouTube Red

YouTube Red (1 month free trial)

$144.99

This email confirms your subscription purchase:

Subscription	YouTube Red
App	YouTube: Watch, Listen, Stream
Content Provider	Google, Inc.
Date of Purchase	23 January 2018
Price	$144.99/month
Payment Method	By Card

You will not be charged for your free trial. Once it ends, your subscription will renew at $144.99 unless you cancel by 28 February 2018.

To cancel subscription go to, Subscription/%E-mail_address%/VOID-y88q92.

Regards,
The App Store Team

For answers to frequently asked questions, visit Apple Support.

Privacy: We use a Subscriber ID to provide reports to developers.

Apple ID Summary • Terms of Sale • Privacy Policy

Copyright © 2018 Apple Inc.,
All rights reserved