* Employees at your company have started receiving daily calls from an estate executor company requesting their PayPal information in order to claim their $1,000,000 inheritance from a distant Ukrainian relative. At the same time, new employees have been complaining about $50 missing from their biweekly paychecks and have been finding strange emails in their inbox from a former janitor, who was fired a month ago because he played World of Warcraft on the job.  You have heard that the Facilities Services desktop computer runs on Windows XP.

IN A MS WORD DOCUMENT, SUBMIT THE FOLLOWING:

* 1. A root cause analysis of what most likely happened.  You may use Figure 5.5 on p. 133 to help you analyze the situation. (10 points)
  2. What assets (hardware, software, data, etc.) are impacted?  Classify them in a table like the one on p. 134 of your book and determine the “primary” asset (i.e. the asset central to the system, with all other assets supporting its existence).  Then rank the other assets based on their sensitivity and criticality and explain your ranking. (10 points)
  3. Determine and indicate in the report any other “hidden” assets support the current, on-site configuration. How does user account information “leave” the CIO’s desk and “arrive” at Human Resources? (20 points)
  4. What can be done to fix this situation in the long term?  Which system needs to be replaced?  Would you recommend IaaS or SaaS or a local solution?  Why? (10 points)

Company is something which is considered to be a place which does good to the clients and also society, but there said to be considered to have many loop holes which makes the people interpret the happiness of client and people who are working and gain happiness only towards them which starts with jealousy and greed. For a scenario like this it would be always be a non-ideological situation to react but being a risk analyzer it should be a team thinking to anticipate the situation, and ready laws to eradicate such kind of situation. Let see go and see what brought this kind of situation and what kind of assets involved in this, and what best can be given to help the situation, and no not make a organization to fall in such of situation repeatedly.   
  
Organization which consists of call center of inbound center, would always considered to have similar type of calls, so we can have similar type of similar number an inbound manager can deactivate the number from get the organization dialed. In this , any company person reveals any information then data, and in person asset would be affected. We identify in the scenario that people are receiving with emails from ex employee of the organization who was been fired one month ago, so which means the ex employee account was not been de activated by HR department, and where he was having access to mailing list if the employee, so which made him to send email , and which was a kind of data, software, legal information asset. In the other side that in new employee are missing with 50$ pay check from one month, so which means former employee is also having access HR Records, where he was eligible to make changes to record, in turn we identify somebody is helping from HR Department to make things for him, and where we can identify janitor was been removed from a respectful position, which made him as very influential person. Playing game in the working time is something violating organization rules and ethics of a person, because they would not pay for playing games at the office time that to in office. Here is the example, <http://www.wikihow.com/Hack-Windows> how to hack windows xp system, which is easy where steps are also provided all around the world. So being less secure system available in the organization to make a loop holes from the user violating the rules of legal, which means a user was been authorized to make changes to system administrator, to make changes to the system, which means user was been authorized which made Risk Management who had configured the system had made wrong configuration, and brought a loop holes to the organization. In this we consider Student Email Data, Email Server Software, Email Server Hardware, External Storage, Server Hardware Maintenance Agreement, Email Server Software Maintenance and technical support agreement are been violated. As per the Figure, we identify that Bot activity by the user of non-working person, due to access which would not be considered to be as any kind of zombie attacks. Yes, for account Credentials these was account was open even the user was not working for the company where this would be considered to be as a HR Department negligence. Being access to email itself we can have access of how many things he would gain access which interprets with client side certificates. Financial Credentials can also be very easy for the person if the pc is still accessible, and phishing login to email was not been notified to email creator with a message on this, and where it should be the requirement and review the time stamp of it regularly and also missing money from new employees which made him to access to HR Department. Virtual Goods was also very important section where was able to access to operating system license key with email attacks which is internally related to the situation.   
  
Like in this table there said to be considered there said to be many on this, but as of now restricting to 6 points.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset | Asset Type | Sensitivity | Critically | Owner | Responsibilties | Ranking |
| Email | Software Asset | Un Restricted | Essential | HR | HR,IT | 1 |
| HR Records | Information Asset | Restricted | Essential | HR | HR | 2 |
| CIO DESK | Information Asset | Restricted | Essential | CIO | CIO,HR | 3 |
| System | Legal Asset | Restricted | Essential | IT | IT,HR | 4 |
| HR Department person | Information Asset | Restricted | Essential | HR | HR | 5 |
| Inbound call | Personnel Assest | Un Restricted | Deferrable | End User | Customer Support Manager | 6 |

In the above paragraph there are couple of examples which where been identified with hidden assets. The information from CIO Desk to HR has been moved because of what we interpret that there said to be a person who got bend down for money and might helped the person, and janitor might have been removed from a respectful position and he needs to be influential person to get the works done from HR Department.  
  
  
In this kind of situation, We try to give couple of suggestion to organization to make the process more efficient and make it effective for keeping it for long time. Starting from Call Center, people should trained to deliver what content need to be given over phone and so training need to be given in high way. Then speaking regarding HR, if a person leaves the organization, his access to be removed on the day there said to be considered a notice period of the person to leave the organization, and within one day access need to be removed. HR Department need to know the access and authorization limit for the people to access, and if accessed then that should be authorized and have a review of time stamp. CIO team need to give proper authorization, to what people and what work are allowed, and email internally delivered was been reviewed before delivering and then IT Team should create a network which works internally and secure to maintain proper standards not to allow any kind of site loaded externally. These are couple of systems which need to be modified. We would suggest to keep Software as a Service, as a requirement , but we suggest to maintain standards, and then review the results, if the results does not give more effective results, then we can have SaaS which would bring more better results, As on any new technology would take time to get it effective results.