**Name:** CENSORED

**Due Date:** 12/6/19

**Class:** ISMN-5740

**CASE 2**

1. **Executive Summary of my Findings:** I have presented a quantitative assessment on what I believe to be the top 3 risks that are present to your business. The risks I believe to be the most dangerous are Social Engineering, the inability for the current personnel to deploy the needed access controls, and the Transaction Processing Server. While social engineering is what I have determined to cost the most, it is based on a theoretical cost analysis; the current costs to your business are probably low for this risk, although it is a fairly popular attack vector that must be protected against in the future. The risk that I believe to be the most dangerous to the company is the Transaction Processing Server (TPS), which is currently a single point of failure for your business. When the TPS system experiences an interruption, your business cannot continue operations and therefore suffers a loss in profits; this cannot be acceptable in a business and must absolutely be addressed first. The remediation alternative I have decided is the best is a backup TPS system; this will allow your business to almost immediately resume operations if the main TPS experiences an interruption. This will cost anywhere from $100,000 - $500,000 and so will be the second most costly issue to address as well as the most beneficial for your business. Next, the issue with social engineering should be addressed, since it has the easiest and most efficient countermeasures to implement; this will benefit your business in the long run and not take a large amount of manpower or difficulty to implement. The remediation alternative I have recommended is to implement spam filters and raise workplace awareness, so the costs to implement these should be in the low $100’s - $1000’s and will take a very short amount of time. Lastly, the issue with IT personnel must be addressed; I have recommended the remediation alternative of hiring the appropriate staff to help employ and moderate the much-needed access controls for your business. This is important to help address all the other issues I have addressed in the first case report that will impact your business financially in the long run.
2. **Cost-Benefit Analysis (CBA):**
   1. Social Engineering (Previous Top Ranked Risk):
      1. Losses Expected Before/Without Countermeasures: Your business could go bankrupt depending on the strength of the social engineering attack and what they target (i.e., unauthorized access to the Customer SQL database, an in-branch terminal or one of the many important servers could bankrupt the company if the damages are severe).
      2. Losses Expected After Countermeasures: The countermeasures can keep the damage costs very low if one of these attacks are successful but cannot control legal fees that may result from a successful social engineering attack.
      3. Annual Projected Benefits: The company will benefit from the countermeasures by saving money that could have been spent on damages (and will overall save money because the frequency of these attacks will decrease). This can be shown with the formula “loss before countermeasures” (bankruptcy or close) – “loss after countermeasures” (low to medium cost, or none at all depending on the type of countermeasures chosen) = “projected benefits” (which in this case would be a very large number, since we cannot appropriately assign cost values for this type of risk).
      4. Initial Cost for Countermeasures: The countermeasures to protect against this attack will initially cost somewhere in the low $100’s range for the needed software if the first remediation alternative is chosen, or $0 if the second is chosen.
      5. Annual/Recurring Costs for Countermeasures: Things like antivirus software and spam filters may have a recurring cost, but the combined costs should be in the low $100’s range (the annual cost is still zero if the second remediation alternative is chosen).
      6. Value of Countermeasures: The countermeasures are monetarily not worth much but will be worth a large amount to the company by saving money. This can be shown with the formula “projected benefits” (which we determined is a very high number earlier) – “cost of countermeasure” (which we have determined to be in the low $100’s initially and annually, or $0 if the second remediation alternative is chosen) = “countermeasure value” (which will, again, result in a very large theoretical number).
   2. IT Personnel Risks:
      1. Losses Expected Before/Without Countermeasures: The industry average for fines related to customer data breaches was (last year) $100,000 per breach. The average amount of breaches per year is low, but the impact of each breach is very high so the losses would annually be in the $100,000’s without countermeasures.
      2. Losses Expected After Countermeasures: The cost per breach will likely still be the same (although it might generally be lower if less customer data is exposed as a result of the countermeasures). The amount of breaches per year for this company should be below the average if the countermeasures are accurately implemented, so the overall amount of losses will (usually) be less.
      3. Annual Projected Benefits: We can find the annual projected benefits with the formula “loss before countermeasures” (which we determined to be higher than the losses expected after countermeasures) – “loss after countermeasures” (which should be lower than the loss before countermeasures, if not 0) = “projected benefits” (which should be relatively high in the $100,000’s range).
      4. Initial Cost for Countermeasures: If the first remediation alternative is chosen, the cost will be high (in the high $100,000’s) for the new staff members and access controls; if the second remediation alternative is chosen, the cost will be low (in the low $1,000’s) for the training of the current IT staff combined with the countermeasure costs.
      5. Annual/Recurring Costs for Countermeasures: If the first remediation alternative is chosen, the cost will be high (in the high $100,000’s) for the staff member salaries combined with any annual fees that might come with the access controls; if the second remediation alternative is chosen, the only annual fees will be from some of the access controls (which should be in the low $100’s).
      6. Value of Countermeasures: The value of the first remediation alternative can be found with the formula “projected benefits” (in the $100,000’s) – “cost of countermeasure” (which is also in the $100,000’s) = “countermeasure value” (which is a low or negative number); the value of the second remediation alternative is “projected benefits” (in the $100,000’s) – “cost of countermeasure” (in the $1000’s) = “value of countermeasure” (which will be really high in this case).
   3. IT Infrastructure Risks:
      1. Losses Expected Before/Without Countermeasures: An average of 5 interruptions with an average duration of 4 hours can be expected before/without countermeasures; the provided estimation of losses per hour is $25,000, so it can be estimated that your business will lose an average of $500,000 per year.
      2. Losses Expected After Countermeasures: The countermeasures will mitigate the TPS from being a single point of failure, so there should (ideally) be no further business interruptions due to this system being compromised.
      3. Annual Projected Benefits: We can find the annual projected benefits with the formula “loss before countermeasures” (which we determined to be $500,000 per year on average) – “loss after countermeasures” (which we projected should be $0 per year) = “projected benefits” (which should be saving an average of $500,000 per year for your business).
      4. Initial Cost for Countermeasures: If we are going with the first remediation alternative (purchasing a backup TPS) then the initial cost will be between $100,000 - $500,000; if we are going with the second remediation alternative (purchasing a hot site that can be close to your business) then the initial cost will be about the same.
      5. Annual/Recurring Costs for Countermeasures: If we are going with the first remediation alternative (purchasing a backup TPS) then the annual cost will be in the $1,000’s; if we are going with the second remediation alternative (purchasing a hot site that can be close to your business) then the annual cost will be in the $10,000’s.
      6. Value of Countermeasures: The value of the first remediation alternative can be found with the formula “projected benefits” (in the $500,000’s) – “cost of countermeasure” (which can be anywhere from $100,000 - $500,000) = “countermeasure value” (which can be anywhere from $0 - $400,000); the value of the second remediation alternative is pretty much the same. The difference in the values of these countermeasures is the annual costs that will occur as a result of using each one; the annual costs will be less if we go with the first remediation alternative.
3. **Remediation Alternatives:**
   1. Social Engineering (Previous Top Ranked Risk):
      1. Social engineering could be partially remediated with antivirus software on every machine, spam filters for e-mail accounts, and 2-FA authentication for logins that could be accessed by a third-party.
      2. The other alternative to remediate this risk is to raise workplace awareness on this issue; moderate employees, have reminders posted in the workplace that help identify social engineering attempts, offer rewards for reporting phishing emails, or do anything else that may help employees prevent these attacks from affecting the company.
   2. IT Personnel Risks:
      1. Access control specialists can be employed (even if it is only temporary) that can help design, implement, and monitor compliant administrative, technical, and physical access controls; this will generally cost your business a decent amount of money (for the access controls themselves, to pay the specialists a salary, etc.).
      2. Training seminars, workplace research teams, and online tutorials can help the IT staff design, implement, and monitor compliant administrative, technical, and physical access controls; this will be the less costly and less efficient remediation alternative. The current IT staff can be trained to handle (at least some) of the access controls that are required for your business.
   3. IT Infrastructure Risks:
      1. A backup Transaction Processing Server (TPS) can be purchased so that operations can almost immediately resume in the event of an interruption within the main server; a backup server can cost anywhere from $100,000 - $500,000 and may have annual costs (but they would be in the $1000’s).
      2. Your business can invest in a hot site so that business operations can be moved and resumed at the new site; this would be about the same initial cost as the first remediation alternative, but it may have higher annual costs (somewhere in the $10,000’s per year).
4. **Remediation Recommendations:**
   1. Social Engineering (Previous Top Ranked Risk): I would recommend going with the second remediation alternative; while the first will be helpful in dealing with certain aspects of social engineering, the most overall benefits will come from teaching employees to be aware of this type of attacks. Another reason that this should be the preferred remediation alternative is because the cost to implement it is $0, since workplace awareness is easy to implement without spending any money (although some money can be beneficial if used for training seminars, social engineering simulations, etc.).
   2. IT Personnel Risks: I would recommend going with the first remediation alternative; while the second will save the company from large costs, not every risk can be appropriately mitigated by the IT staff (no matter how much training they go through) so the company will still lose a large amount of money per year to breaches. The first remediation alternative, while more costly, will help secure the company from breaches in the long run. While breaches cannot be completely avoided (it is impossible to completely protect a company from a breach), the annual damages (and costs) will be less than they would be with the second remediation alternative or if the company did nothing. It would be more beneficial if a mixture of these two remediation alternatives were chosen; some access control specialists can be hired for the very difficult access controls, and the rest can be handled by the IT staff after some training.
   3. IT Infrastructure Risks: I would recommend using the first remediation alternative; this is because it is cheaper annually and it can cause business operations to resume sooner than if your business had to relocate to a hot site (even if it is a relatively close distance from your business). This would allow business operations to run in a timelier manner and be easier to resume in the event of a TPS interruption.