Chapter 8:

1. **What processes need to be in place to effectively establish IT project priorities?**
   First, a process needs to be owned by business units who contribute a representative with decision-making authority so that the consequences are shared between IT and business. Second, the process should have transparency and vision of decision consequences. Third, the participants must maintain some continuity and within-project focus.
2. **Is assigning control of IT budgets to user departments and effective mechanism to establish IT priorities? Who should control the IT budget?**
   Yes, I believe it is, as IT knows better of their priorities than the business department. I think IT should control the IT budget as they have a better sense of where money and resources should be put in their department as to prevent further issues down the road, such as the security example in the chapter. The business department might overlook it or see it as a low priority since it does not affect present business but if the problem grew it would be an issue later on. This is something that is more apparent to the IT department than the business and loans department.
3. **Given his disagreement with Maggie and his peers, do you think Barton is wise to ask for IT budget control? What consequences (positive and negative) do you foresee?**
   I think it is still wise for Barton to ask for control, especially in his case because he has a business background so he knows how to handle the money. The issue with the last CIO was he was all IT and no business. But this time Barton has a business background and he is becoming more informed of the IT side of things. This shows that he would use the budget wisely and more appropriately than someone who knows nothing of IT. I think a positive consequence would be that IT now has the resources they need to go ahead with project they deem to be an issue and not have to try and convince the business department for the funds. A negative consequence I see is that if they spend the funds on a project that Barton approved and it failed, then the whole blame would be on IT. But more specifically the blame would be on Barton, since he decided to take control of the budget and allocate resources. That’s a lot of responsibility for one person.

Chapter 9:

1. **Why do you think the IT presentation at the board meeting was scheduled as the last agenda item and given only thirty minutes?**
   I believe this was the case as board members do not want to concern themselves with IT too much. Like they said, “stay in the basement where it belonged”. Board members would rather IT just be told what to do then go do it. Additionally, often times meeting run longer than expected so this would give IT even less time to talk about their department than 30 minutes. They would have to cut themselves off mid-presentation if the meeting ended since they are the last agenda item. This is a benefit to the board members who do not want to get involved in IT matters.
2. **What are the board of directors’ responsibilities with respect to IT oversight?**
   The goal of IT oversight would be to be more knowledgeable about IT risks which is mostly invisible to managers until that risk becomes a reality. With a board committee for IT oversight, these potential risks will be monitored more closely and often so that board members are more involved. Other responsibilities would be going over the additions and evolved complexity of

infrastructure as risks develop incrementally. So, if there are board members watching the increments along the way, they will be more informed of the risks that are there.

3. **Why do you think they seemed eager to delay forming the IT Oversight committee until the next morning?**
   Often times, people want to stay away from areas they are not comfortable with. In this case, most of the board members had little to no experience in IT. If the meeting went on, then they may be asked to serve as part of the IT committee which most of them did not see comfortable with. By delaying the meeting till the next morning, it also gives board members time think about the IT Oversight committee that they may have to be a part of and what will be required of them and if they're up for the task. Board members seem to have been comfortable with their roles up till now because it was in their wheelhouse but as times change, not knowing anything about it will no longer be a valid excuse.
4. **What should Barton do about "managing Carraro"? Managing Williams?**
   I believe Barton should try to make Carraro an ally but also continue giving updates to Williams as he is his boss and he gave him the position of CIO. This would bring up the assumption that he can take it away too. Makin Carraro an ally would be wise as it may also help to convince the other board members in the pursuit of forming and IT Oversight committee or being on Barton's supporter in future IT decisions. However, if Barton started leaving Williams out of the loop of what Carraro and him are working on then it may prove harmful for Barton. So Barton should manage Carraro as an ally and supporter, and manage Williams by keeping him in the loop and updating him on all the work going on between them.
5. **How is Barton doing after almost three months as IVK's CIO? What is your assessment of his performance?**
   Barton is doing more already than I believe past CIOs have done during their time at IVK. Since Barton has had prior business experience, he is able to relay the information of what IT needs more effectively. Rather than Davies, for example, who had not so much business experience so it made it harder for him to get projects approved as the business and loans departments didn't understand the need for it. Barton is able to be the bridge between IT and business more efficiently than any person prior (to our knowledge). It seems he has the highest ratio of getting things done within his time spent as CIO than people filling the role previously. So, my assessment would be that he has proved successful at his new role only within a few months with little to no IT knowledge and if he kept it up, he could definitely take Williams' position one day, which makes sense for Williams to be concerned about.

<u>Chapter 10:</u>

1. **How should Barton handle the meeting with the analysts? What questions should he be prepared to answer and how should he answer them?**
   I believe Barton should continue to talk about financial status of the company and try to stay on that topic for the analysts. It's best to avoid disclosing information regarding the outage especially when the company does not have all the information. However, Barton should be prepared to answer questions about the outage honestly with the knowledge that he has about so that he discloses everything legally. He should do it in a way though that reassures the analysts that the company is getting back on track and the issues are being fixed as they speak.

2. **How vulnerable is your company (or a company that you know) to a denial of service (DoS) attack or intrusion? What should be done about such vulnerabilities?**
   A company can be extremely vulnerable to an attack or intrusion due to lack of updates or maintenance on security systems of the company. This can also happen due to lack of resource allocation to security projects. These attacks and intrusions could have severe negative consequences including client information being stolen which will lead to legal complication. This will prove to be an expensive mistake. These vulnerabilities can be avoided by providing appropriate resource allocation to IT projects that work on security issues. Additionally, the security systems should be continuously checked to monitor any updates it may need as the infrastructure becomes more complicated and larger as the company grows.
3. **Why can't perfect IT system security be achieved? If security can never be perfect, how should you manage against malicious threats?**
   IT systems can't be perfect because it would require infinite investment. Security problems are not a single factor, but rather the emergent result of countless incremental and individually harmless decisions. Sometimes these decisions are used for customer satisfaction such as faster database access time, but you may end up making the connection to the database more exposed. You have to give something to get something, especially with large complex company infrastructures. You can manage against malicious threats by providing appropriate resource allocation to security projects or a constant monitor and update on your security system so that the company has the latest security measures implemented to prevent against malicious threats.

Chapter 11:

1. **Which option for securing IVK in the aftermath of the security incident would you choose?**
   I would choose the option where IVK shuts down the company, except operations that could run manually, as soon as possible and rebuild critical production systems from development files. I believe this to be the best compromise between time, money, and legal issues. Doing nothing would make IVK severely at fault for not disclosing anything in the chance that client information was taken. Creating a mirror site and rebuilding production system is both costly and time consuming. Not to mention that something else bad can happen during the time it takes them to get the mirror site up or even if they did nothing. That's why the option to shut down parts of the company is best because it avoids anymore leak of information in the event there is a bad guy, and it is quicker and cheaper to use this method than the mirror site.
2. **What would you disclose?**
   I would disclose, with the option I chose above, the recent attack that had happened to specific clients whose information was most recently accessed as it is most likely that their information is most at stake. This way, it does not alarm all the clients or put a statement to everyone that IVK in incapable of protecting client privacy. By reaching out to a few clients to be cautious, they abide legally and ethically to the attack and with respect to their client. They don't know if there is a bad guy for sure, but it is better to be safe than sorry in my opinion. Telling them when it's too late will not help their case. Disclosing nothing would make it unethical and put them at risk of legal consequences. However, they should disclose this information with reassurances that they are working around the clock to secure their system and not let anymore information leak.

3. **Did CEO Williams make the best decision for IVK? Why didn’t Williams fire Barton?**
   I don’t believe he did make the best decision. This would be the best decision in the case that there is no bad guy, but with the evidence given of the gotcha emails and the filename change, it would be likely that there is a bad guy. Williams chose to hide the attack and not disclose it, but if bad guys did end up taking information and they concealed this information from clients, it will be very bad for IVK down the road. Keeping up images is important to Williams, but IVK’s image will be completely destroyed if the attack ends up being more malicious than they thought. And concealing the information won’t help. I think William’s didn’t fire Barton because his good points outweighed his bad points. Even though there was this huge outage, Barton still performed well for 3 months, achieving much, and he handled the analyst meeting well. Also, Williams had just fired the head of Loans Operation, and Barton previously held that role. Firing both people fit to lead Loan Operations would be unwise as then he would have to fill the role of CIO and head of Loans Operators.