IA2 – Operating Mistral Bank

David C. Shields

CSEC 670, Section 9041

Contents

1. Introduction 3
2. Briefing for the Briefing 3
3. Being the Bank – Simulations 5
3.1 Round 1 – Phish Food and Hacktivists 5
3.2 Round 2 – Tanking Economy and Worms 7
3.3 Round 3 – More Phishing and the Empty Trojan 8
3.4 Round 4 – Hacker! No Hacking! 10
4. Team Thoughts 11
4.1 Team Leadership 12
4.2 Team Motivation 12
4.3 Team Conflict Resolution 13
5. Lessons Learned 14
6. Summary & Conclusion 15
7. References 16

1. Introduction

One of the most common drawbacks in a formal education program is that the student learns concepts but does not have real-world experience executing the concepts learned. In other words, one of the most common arguments against attaining a higher education is that the students have theoretical knowledge in a discipline but not in its execution. In the case of the Cybersecurity Capstone course at the University of Maryland University College (UMUC), the story is very different. Students are challenged with running a virtual company in a virtual world and must respond to attacks that are based off real-world security issues. In my case, I was chosen to serve as the Chief Information Officer (CIO) of Mistral Bank, a large financial company. Throughout the simulation, I worked with a team of students to create a strong cybersecurity infrastructure and defend against attacks that a major bank (or any enterprise) might actually face in the real world. To succeed in the simulation, it was necessary to research the industry, study technical controls, apply controls and work as a team.

2. Briefing for the Briefing

Before one can be in charge of a bank, or any organization for that matter, one must understand the industry and the companies against which it competes. Prior to the initial simulation, the team at Mistral Bank had to create a sector briefing. In the briefing, I was tasked with researching the history of the banking industry including notable hacks in recent years. Additionally, I needed to research the federal structure behind banking to properly grasp the ecosystem that controlled the banking industry. After thorough research and investigation, I collected so much information that I actually had to limit the amount of information I discussed in my portion of the paper because it would have spanned several additional pages otherwise.

There is no doubt that reviewing the countless webpages, studies and government documents provided me with a more clear understanding of the banking industry. I had prior knowledge of the financial industry because of a brief contract position working for a local bank but to see the entire framework of the government portion – the Federal Reserve, the US Treasury, Office of the Comptroller of the Currency and various others – makes it very clear how deeply regulated and highly resilient the banking sector in the USA has become. Collecting all of the information was very important in helping me have a deeper grasp of the task we were up against at Mistral.

Once the team had completed our Team Sector Briefing, we still had another task at hand – lining out the roles for the team members to take. We had five people on our team and we needed to properly organize the responsibilities for 32 simulation controls. The team had a meeting where we discussed the interplay between each control and the type of leadership structure that we wanted to implement for Mistral Bank. We decided upon the following structure:

Table 1 – Mistral Bank Organizational Roles

Team Member	Organizational Role
Dave Shields	Chief Information Officer (CIO)
Joe Schott	Chief Information Security Officer (CISO)
Aaron Rivers	Controller
Brandon Rutledge	Information Assurance Officer (IAO)
Patricia Schuetz	Vice President of Human Resources (VP of HR)

The Chief Information Officer's role was determined to be the person in charge of the global project view as well as the person who would manage all decisions related to technology. As a result, the CIO originally had the authority over Authentication, Backup, DNS Redundancy, Load Management, Patch Management, and Virtualization or Cloud Computing. The CISO's role was going to focus on the policies behind the information security framework and was originally given the controls: Antivirus Policy, Authorized Software Policy, Firewall, IDPS, Physical Security, Remote Access Policy and Information Sharing Policy. The Controller would focus on the financial side of the house and would serve much like a CFO which would have made his controls: Advisory Subscription & Federal Help, Database Security, Financial Security Measures, Information Sharing, SOX and GLBA, and training and auditing. As the name suggests, Mistral wanted our Information Assurance Officer (IAO) to be responsible for Continuity of Operations in the event of a disaster or breach and to be responsible for the communications with the public in the event of things such as service outages so our IAO was assigned: Breach Notification Policy, Business Continuity Planning, Emergency Bypass Policy, Public Relations, Role-Based Access Control and Systems Development Testing. Finally, our VP of HR was to be responsible for the 'people matters' of the company so the role was to control:

General Access Policy, Hiring & Employee Policy, Information Privacy Policy, Insurance Policy, Training, and Training Incentives. Mistral was ready to take on the cybersecurity simulator.

3. Being the Bank – Simulations

The team finalized our roles and controls for the simulation round but ran into an unforeseen challenge. Both Joe and I discovered that we were not able to select all of our controls. We could reach the maximum limit of 6 controls, but he and I had been assigned 7 controls. After a considerable amount of trial and error, we determined that the simulator had a flaw which would only allow the first two students in alphabetical order by first name to select more than 6 controls. The system flaw meant that both Joe and I would have to each give up one control and give the control to either Aaron or Brandon (the first two names, alphabetically, on our team). In the end, I gave my control of virtualization or cloud computing over to Brandon, our IAO and Joe gave his control of the Information Sharing Policy over to Aaron, our Controller. The team entered its controls in to finalize them and the first round began.

3.1 Round 1 – Phish Food and Hacktivists

The first two challenges that Mistral Bank faced in the simulation were a phishing attack that only affected Mistral and a hacktivist attack that impacted all the teams. In order to make the best decisions possible, I needed more information about what a split DNS topology entailed and I needed a refresher on what RAID6 was as I had primarily dealt with RAID5 in my professional experience. After reviewing a chapter in the Computer and Information Technology Handbook by J.R. Vacca, one of the first books I acquired in my courses, I was able to determine that the DNS redundancy and the Split DNS topology would be critical ways to protect our company against hackers and other security threats since they strengthened our network against outside attacks (Noble, 2009, p. 699). My answer to RAID 6 came after reviewing a storage library site – I wanted RAID6 as well.

I began to insert my decisions into the simulator when I realized that I had misunderstood what delayed binding was used for and required a pause to research the topic as well. After reviewing the university library server, I found a useful academic report from 2012 that discussed the use of delayed binding as a technique to prevent TCP SYN flood attacks

(Saravanan & Gowrishankar, 2012) which I had previously read was a common attack used by groups such as… hacktivists! I now felt that I had made the decisions I wanted to make and I also felt that I had strong academic research and personal experience to support my decisions. The controls changes that I made in the first round are outlined in Table 2 below.

Table 2 - Round 1 CIO Decisions

Control Domain	Control Decision	Value
Authentication	Kerberos Server Spending	$300,000 of 400,000
	Key Distribution Center Spending	$20,000 of $25,000
Backup	RAID Level	RAID6
	Hot site maintenance spending	$300,000 of $400,000
	Remote Backup spending	$15,000 of $20,000
Data Encryption	Level of Encryption	Drive
DNS Redundancy	DNS Server Redundancy	Yes
	Split DNS Topology	Yes
Load Management	DDOS Protection through delayed binding	Yes
	HTTP Security through load balancing	Yes
Patch Management	Frequency of patch Management	Critical and important updates
	Degree of testing prior to installation	Medium
	Trustworthiness of patch	Official

I submitted my decisions and my justification for the decisions in a table to the rest of the Mistral Bank team and they all enjoyed the structure so much that it became the standard used by the team to report our weekly decisions. As a team, we had a teleconference where we all were responsible for voicing our decisions and supporting them if any other teammate disagreed with

the decisions. Once we all agreed on the decisions, they were entered into the simulation and we waited for the results.

Mistral Bank did not do as well in the first round as the team would have hoped but it was a great experience to see how the team performed under pressure. We agreed to split out the work on our post-simulation report such that each team member supported their decision as they were required to do in the team meeting and we divided the paper writing work accordingly. Fortunately for my decisions, the choices that impacted us in a negative way were more related to the non-technical areas of the simulation such as public relations and employee morale so I felt that I had performed as well as could be expected. The first round was over and now the second round would begin.

3.2 Round 2 – Tanking Economy and Worms

When the second round of the simulation began, the challenges were much more difficult than the first round and, unlike the first round which was divided into two weeks, we only had one week from start to finish for Mistral to prepare. The biggest challenge we faced in the second round was the economic downturn as there was very little our team could do to defend against it. The second round also featured a worm attack so the Mistral team worked hard to protect against the one attack we could actually defend against.

Before the first day of the new week had passed, I had already decided on the control changes I wanted to make. I knew that the worm attack had the potential to cause downtime to the bank so I opted to increase the two controls that I felt were most likely to be useful. I increased the spending on our hot site maintenance to the maximum of $400,000 and increased remote backup spending to the full $20,000. The decisions list was smaller than the last one but the rest of the team used my table decision document as a basis for their decisions.

Table 3 - Round 2 CIO Decisions

Control Domain	Control Decision	Value
Backup	Hot site maintenance spending	$400,000 of $400,000
	Remote backup spending	$20,000 of $20,000

During our week two team conference, Joe introduced the team to the Capstone Simulation Application Model Reference and helped us understand how our decisions could impact the simulation rounds. To be honest, I had downloaded the document when it became available but due to my inexperience with the simulation at that time I had only skimmed the document and had no idea how useful it would be. I also felt that the team did not have a good way to calculate our success/failure rate by simply reading our feedback so I used the custom reports function in the simulator to create what I called the index document to show our scores and compare them with the average of other teams and help us more clearly determine our deficiencies and our strengths. I introduced the team to the index document at the week 2 conference and it was met with much approval and fanfare from the team and aided us in approaching our 'Lessons Learned' section of the team simulation reports.

When the simulation round was completed, Mistral took another major hit to our customer satisfaction and employee morale thanks to the economic downturn. Thankfully, the worm did not reach us. We were reassured by the success that we were doing the right things from a technical security standpoint. The team determined that we wanted to make Mistral Bank into customer service maniacs and improve our employee morale as the next round approached. Overall, we did well on our profitability so we had enough financial support to apply to those areas – especially since our technical security values were so high. The first half of the simulation was over and our team prepared for the third simulation round.

3.3 Round 3 – More Phishing and the Empty Trojan

As Mistral began the third round, we were surprised to see that our bank was once again targeted for phishing attacks and we also had to determine the best way to prepare for the onslaught of the Trojan. After a thorough analysis of the tools I controlled, I decided that I did not feel it was necessary to change any of the controls I was responsible for. The phishing attacks we faced in round 1 had largely been impacted by public facing controls which I had no control over and therefore the situation could not be helped or hampered by my choices. Furthermore, the internal and external security control scores had been some of the highest scores for our team over the past two rounds and I felt that increasing the expenses for my technical controls would only cause unnecessary use of funds – something our team did not have much room to risk.

During our team meeting, it became apparent that although we had access to the Application Reference Model, it was very challenging for the team to visualize how their controls had any impact on our scores at all. Since I had no control changes to support during round 3, I agreed that I would use my index-generating powers to create a decision index that would make visualization much easier. The team agreed that the decision index was a terrific idea and that they would not make their control changes until they had received the document. I created a document that featured every control decision for Mistral Bank and its value range, a numerical score similar to a risk index that expressed how 'strong' the decision value currently established was in comparison to the maximum control value and I connected each decision value to the person on our team who was responsible for the decision. The team had determined that Downtime, Morale, Customer Satisfaction and Reputation were our lowest values so I created a second decision index that showed only the control values that the reference model connected to our low scoring areas. The result was a numerical indicator of the exact controls that impacted our scores. An example of the satisfaction index is presented below.

Figure 1 - Decision Index Sample - Satisfaction

Training		
Focus on phishing training by target	3	Patricia
Focus phishing training on CC fraud	3	Patricia
Investment training for fraud investigation	2	Patricia
Information Sharing Policy		
Degree of external information sharing	2	Aaron
Breach Notification Policy		
Degree of openness of breach notification	4	Brandon
Information Privacy Policy		
Privacy program investment spending	2	Patricia
Appoint a dedicated Privacy officer	4	Patricia
Privacy training spending on employees	2	Patricia
SOX and GLBA		
Degree of customer-end SSO implementation	4	Aaron
Quality of third-party providers for CC/Checks	3	Aaron
Financial Security Measures		
Frequency of CC usage Security alerts	2	Aaron
Mode of reception	2	Aaron
Security questions rigor	2	Aaron
Account lockout procedure rigor	2	Aaron

The team was extremely satisfied with the decision index and expressed that it was exactly what they needed to help clarify their decisions. Based off my model, the team made the decisions that they felt were most important in the simulation and supported it accordingly. The only downside is that I had not made the decision index sooner.

When the simulation round was complete, the team still took a major beating in the areas we had attempted to improve the most. However, after comparing the results with those of the other teams, we determined that the team actually did better than other sectors in the simulation as a whole. We were not impacted by the Trojan attack at all which proved that Mistral was doing a great job from a technical security standpoint. The VP of HR, Patricia noticed that Avisitel and Hytema had done a great job in employee morale and productivity and agreed that collaborating with these teams would be a useful method for improving our scores in those areas. Now, the final round was ready to go and Mistral had a lot of work to do if we wanted to succeed in the final round.

3.4 Round 4 – Hacker! No Hacking!

For the final round of the Cybersecurity Simulation, the bank was faced with every cybersecurity team's worst nightmare – the potential for a hacker attack on our systems. The team knew that the decisions and results made in the final round of the simulation would serve as a lasting legacy for the team. Not only did our team need to deal with the current issue but also we needed to do whatever was possible to recover from previous issues such as downtime. After thinking through my choices and reading up a little about the interplay with Kerberos and the Key Distribution Centers (KDCs), I decided that I needed to increase the power on both controls to reduce our team's downtime (Sandhu, Hadley, Lovaas, & Takacs, 2009, p. 28.10). My final decisions are outlined below:

Table 4 - Round 4 CIO Decisions

Control Domain	Control Decision	Value
Authentication	Kerberos Server Spending	$400,000 of $400,000
	Key Distribution Center Spending	$25,000 of $25,000

In the previous weeks, the team had been holding meetings on Thursdays, two days after the results from the round had been completed and this meeting was mostly used for the team to prepare for the paper. In the final week however, we agreed to move our meeting back to the Tuesday before the simulation round so that we could truly organize our thoughts on how to best compete in the final round. I completed the decision impact indexes to show the various areas of

improvement and no decisions were finalized until all team members agreed to the decisions that each teammate was going to make. In hindsight, the group supported decisions would have been useful in previous rounds but as the old adage from Billy Wilder says 'Hindsight is always 20/20'.

At last, the decisions were made, the controls were updated and the final round of the simulation had run its course. Upon reviewing the final results, I was overjoyed to see that the major threat, the hacker access, had been avoided entirely but was further dismayed that we still suffered from many of the same things that had plagued us before – customer satisfaction and employee morale. Before I expressed my findings to the team, and prior to preparing the final simulation document, I delved into something that I had previously only glanced at – the cross team impact. Reviewing the findings there, I was able to confirm that a majority of the major score decreases in round 4 were the result of the other teams, not Mistral. One example was the score for Popular Sentiment which had dropped 9 points in the final round – I determined that the Federal Government's scores in round 4 had caused a 10 point drop in our team's score. The finding meant that Mistral's controls were such that we actually performed well enough in the popular sentiment to absorb all but one point of the impact from the government decisions. Similarly, our customer satisfaction dropped 5 points thanks to downtime at DTL Power and our network load dropped 6 points due to the impacts of both DTL and Avisitel. In the end, a majority of the drops Mistral faced in the final round were at the hands of other teams.

In order to make sure that our team could properly synthesize the drops in our scores due to cross-team impacts, it was necessary for me to modify both my score indexes and my decision indexes for the final round. When I submitted my findings to the team, we realized that we actually had performed as well as possible in round 4 so we had something to be proud of. We summarized our team findings in the final paper and changed our final section from "Plans for the Next Round" to "Plans for the Future" where we hoped to illustrate the legacy we wanted Mistral Bank to have in the future. The final round was completed and most of us actually felt somewhat sad that our simulated company was now at an end.

4. Team Thoughts

After completing the final round of the simulation, there is no doubt in my mind that it is one of the closest examples of a real-world scenario in cybersecurity that a college can offer students

shy of requiring internships with major companies. The team I was assigned to and the scenarios to which we had to respond require a great amount of teamwork, board meetings, and countless emails – exactly like the leadership teams of major companies! I know for a fact that companies perform this way as my previous employer was a large energy company and I was stationed in its corporate headquarters so I saw plenty of notes from board leaders, news conferences, and email chains, etc. I certainly had many team experiences of note but they can be summarized into three areas: leadership, team motivation, and conflict resolution.

4.1 Team Leadership

The power of a company and the power of a team are directly proportional to the leaders of the company or the team. I have always been a bold person with a flair for leadership, a desire to be in control, and exceptional communication skills. As a result of these traits, I have often worked best in situations where I was responsible for the results of an event or action and I drive for results. I established my leadership prowess early in the team by trying to get the team communicating and organizing for the simulation as soon as I had been assigned a team. Truth be told, I mostly wanted to get ahead of the group project as I have been on other group projects with the UMUC program that did not perform as well due to lack of preparation. I communicated with each team member via email to get a metering on their level of responsiveness and their drive for action and found that I seemed to be the most driven individual on the team but Joe and Patricia were also potential leaders. After our first team meeting, the team unanimously elected me as the leader even though I did not specifically ask to be the leader. I agreed to lead and maintained that role throughout the project. I did share my leadership as often as possible and sometimes scheduling conflicts and other issues required me to depend on other people in the team to act in my absence. Overall, I used my leadership skills to drive the team but I still let both Joe and Patricia share the spotlight with me on a few occasions. In the end, all of our team agreed that we had strong leadership and the motivation of those leaders drove us all to perform well.

4.2 Team Motivation

When dealing with a team of individuals with their own lives, schedules, and issues, motivation played a key role in our ability to function as a team. I learned early on that Aaron often let himself become preoccupied with other activities when he should have placed priority

on reaching various goals that he agreed to. I also learned that Brandon, while an intelligent person, also had a tendency toward procrastination. Throughout the course of the project, I often found Joe, Patricia, and myself doing whatever we could to motivate Aaron or Brandon to complete various milestones. Not only did the use of positive motivation for Aaron and Brandon aid in keeping them on track but we also motivated each other even when performance was not suffering. I feel that our team morale remained stable and even high for most of the project because we all did our best to motivate each other to perform. Granted, motivation alone will not make the team succeed; sometimes there must be a little conflict and naturally – conflict resolution.

4.3 Team Conflict Resolution

Even in the most amazing companies and the most cooperative environments, a healthy amount of conflict is necessary – this includes co-worker teams, sports teams and even marriages. Despite the generally motivational culture we tried to foster on the Mistral Bank team, there were a few conflicts that needed be resolved throughout the simulation. The first and most memorable occurred in Round 1B when Brandon failed to turn in his completed portion of the paper until 3 hours before the completed paper was due. The rest of the team had spent most of our Saturday busily working away at our paper, making edits and trying to finalize but Brandon had not been at the team meeting that week nor had he even emailed us to let us know any status on his work. Finally, he provided his portion of the paper and we hastily edited the portion and joined it with the rest of the paper. When I asked Brandon what had taken him so long, his honest answer was ‘I work best under pressure’. I explained that while I understood that everyone has their own way of working, we really needed him to work at paper completion sooner. After a few less than stellar peer evaluations and even my own consultation with the course instructor regarding the behavior, Brandon finally began turning his work in within a more reasonable time frame.

In another instance, Aaron had provided his portion of the paper well ahead of the schedule but a review of the paper showed that he had essentially copied his prior week’s paper section, changed the ordering and words in a few areas and resubmitted the same information. When Joe and I brought the wording issue to Aaron’s attention, he apologized and said that he had intended

to change more of the wording but had forgotten to do so. Overall, the team was able to handle conflict in a professional and effective way and the entire team grew stronger as a result.

5. Lessons Learned

At the completion of the team simulation project, I still believe that the project was a terrific method to emulate real-life situations that any of the students may face if employed in a leadership position when they complete their degree. The simulation has helped me gain a broader understanding of not only the technical side of cybersecurity but also the management of cybersecurity infrastructure. IT security teams will frequently seek out the strongest or 'coolest' technology when the engineers make the decisions but to be able to understand the executive perspective is a very different challenge. Executives have to balance the profitability of the company with the cybersecurity technologies that best match the industry and company culture and the task is far more challenging than I previously realized. If I were to limit the things that I learned to three areas, I would have to focus on the importance of planning, team collaboration and cybersecurity as a discipline.

One of the greatest things that the Capstone Simulation project helped me learn was the importance of planning and analysis. There is always a potential to overanalyze or not analyze at all and either could be highly detrimental to cybersecurity and profitability. I learned that planning is important for both short term and long term preparation. A vast majority of IT projects run over budget or completely fall apart due to lack of planning (Montealegre & Keil, 2000) and I can see why. Our team excelled during the project because we were able to work together, follow deadlines, and plan our responses to not only the problems of the simulation round at hand but also the problems that were continuing to plague Mistral from the past. Our first simulation round was extremely difficult because we did not have enough planned to react accordingly but with each simulation round, the information became easier to synthesize and the plans seemed to get accomplished more effectively. The ability to plan effectively is a skill that I am certain will be invaluable in my future career endeavors.

Collaboration within a team is vital to project success and I saw this firsthand during the simulation project. Many of my past employers went to great lengths to stress the importance of teamwork and collaboration but to see the collaborative forces displayed so vividly as our team worked together to not only run the bank but also complete our weekly assignments was truly

rewarding. Regardless of the challenges each teammate faced during the course of the project (working double jobs, funerals, sick children, etc.) every member of the team knew that at least someone on the team was there to assist when needed. I saw the collaborative efforts of the team illustrated by the way Joe, Patricia and I shared our leadership and as each teammate worked with the other to finish paper portions as required. If I was ever called to truly serve as the CIO of a major bank, I would make sure that I surrounded myself with dependable teammates who I could call upon to help me with project demands just like my team – I might even try to make the simulation team my real team!

Lastly, I learned that cybersecurity is a multi-faceted discipline with many moving parts. Cybersecurity is not a clandestine operation and is not just about stopping the bad guy before they break into your system. Every aspect of the operations of Mistral Bank required a thorough interplay with every other aspect of the bank and even with other sectors. I always knew that cybersecurity was much more than just IDPS machines, firewall rules and secure computing policies but I could not quantify the discipline until now. I am certain that seeing the cybersecurity operations from a mile-high view helped me acquire a deeper knowledge of the many ways that cybersecurity impacts information technology and business operations. My goal is to view all future cybersecurity projects and goals from a holistic, multi-faceted approach and I learned this, in part, from my time spent with Mistral in our simulation.

6. Summary & Conclusion

In conclusion, the Cybersecurity Simulation has offered me the most realistic perspective of how a multi-national, high visibility enterprise must handle their cybersecurity infrastructure. I learned a great deal about the financial industry and then I had the opportunity to witness four complete rounds of cybersecurity events that might actually occur in a financial company. I had to manage the dynamics of a complex leadership team with varying goals and personalities in order to secure our company. My project experiences ranged from balancing the budget, dealing with team conflict and even dealing with the operations of a large scale cybersecurity organization. In my time as the CIO of Mistral, I was able to witness the grand scheme of operations in cybersecurity from a perspective that would be impossible in almost any other medium. I believe that I will grow as a professional and take on a global perspective that will allow me to face the future challenges of cybersecurity with skill and determination.

7. References

Menand, L. (2007, February 19). *Notable Quotes*. Retrieved April 26, 2014, from The New Yorker: http://www.newyorker.com/arts/critics/books/2007/02/19/070219crbo_books_menand

Montealegre, R., & Keil, M. (2000, September). De-escalating Information Technology Projects: Lessons from the Denver International Airport. *MIS Quarterly, 24*(3), 417-447.

Noble, K. (2009). Security Through Diversity. In J. R. Vacca, *Computer and Information Security Handbook* (pp. 693-700). Burlington: Elsevier.

Sandhu, R., Hadley, J., Lovaas, S., & Takacs, N. (2009). Identification and Authentication. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer and Information Security Handbook* (pp. 28.1-28.19). Hoboken: John Wiley and Sons.

Saravanan, K., & Gowrishankar, A. (2012). An Active Defense Mechanism for TCP SYN flooding attacks. Pochella, India: Computer Science Archive, Cornell University.