iPremier (A): Denial of Service Attack

CIS 8085

October 25, 2022

Venkat Sabbineni, Ipsa Ojha, Kaustuv Dutta, Swati M. Radia, Jeremiah Warren

Contents

Executive Summary

On the morning of January 12th, 2009, Bob Turley, the recently hired Chief Information Officer of iPremier, an online retailer, dealt with a distributed denial-of-service (DDoS) attack targeting his company. During the attack, Bob Turley, who was in New York at the time, held several phone conversations with his IT team and other company executives. After 75 nerve-wracking minutes, the attack mysteriously ended, leaving iPremier with questions about the nature of the attack and about what to do next.

In this report, we will examine and evaluate the steps taken by iPremier personnel to stop the attack, focusing particularly on the performance of iPremier's CIO Bob Turley. This report will highlight iPremier's operating deficiencies prior to the attack, and it will provide a detailed risk analysis of the threats facing iPremier leading up to the attack. After examining the attack, it will provide a comprehensive list of improvements to iPremier's current operating procedures and means for iPremier to prepare for another attack. This report will conclude with an assessment of Qdata, iPremier's IT service provider, explore alternatives to iPremier's current IT approach, and make a recommendation for iPremier to hire a new IT vendor.

Case Synopsis

iPremier is a web-based retail company located in Seattle, Washington. It was founded by Blake Carleton and Rajiv Narayandas, classmates at Swarthmore College, in 1997. After a successful Initial Public Offering in 1998, iPremier's stock tripled in 1999. However, during the Dot-Com Crash of 2000, iPremier's stock plummeted, and iPremier only survived because of cash it received from the 1999 IPO. As of 2008, the stock has risen again, and the company is narrowly profitable. iPremier's customer base is mainly high-end consumers, and most of their products are priced between $50 and a few hundred dollars. In October 2008, iPremier hired Bob Turley to be the company's next Chief Information Officer.

On January 12th, 2009, Bob Turley, who was in New York for a business trip, received a phone call at 4:31 A.M. from Leon Ledbetter, an IT employee at iPremier. Leon told Bob that the company website was inaccessible for customers and that iPremier's support team was receiving bizarre message. When Bob hears about this activity, he asks Leon if the company had started emergency procedures, but Leon tells Bob that he cannot locate a physical copy of the company's emergency procedures plan.

After his phone call with Leon, Bob calls Joanne Ripley, Leon's manager in IT. Joanne informs Bob that she is on the way to Qdata's facility data center. Qdata is iPremier's IT service provider. Both Leon and Joanne previously told Bob that they had serious misgivings about Qdata, but they told him iPremier did not change providers because management did not identify it as an issue. During their call, Joanne and Bob consider physically pulling the plug on the system, but they opt not to do this. Joanne also tells Bob that the company's business continuity plan was out of data and essentially useless.

Next, Bob spoke to several other iPremier employees. Warren Spangler, head of iPremier's public relations, calls Bob. Spangler discusses the company's stock price and tells Bob he has the PR angle covered. Bob then speaks to Tim Mandel, another IT manager at iPremier. Tim tells Bob not to unplug the system because they might lose the logging information. After his conversation with Tim, Bob spoke to Peter Stewart, the company's chief counsel. Stewart tells Bob to shut down the system.

Meanwhile, Joanne arrives at the Qdata data center, however, Qdata employees refuse to let her into the facility. After hearing this news, Bob asks Jack Samuelson, iPremier's CEO, to call someone senior at Qdata to let Joanne into the operations center. This procedure works, and Joanne enters the operations center. In the operation center, Joanne determines that they are experiencing a DDoS attack directed at the router that runs their firewall service. She mentions to Bob that they need a better firewall. When Joanne tries to shut off traffic from the 20-attack addresses, ten new attackers pop up to take their place. She tells Bob she will call him again if something happens.

At 5:46 A.M., Joanne calls Bob and tells him that the attack stopped abruptly. Bob and Joanne discuss whether the DDoS attack is the work of unsophisticated attackers (script kiddies), or if there was more to attack like an intrusion. Bob asks Joanne to summarize her findings in a report. Now, Bob must decide what to tell the CEO about the attack and what to do next.

Key Question 1

How well did the iPremier Company perform during the 75-minute attack? If you were Bob Turley, what might you have done differently during the attack?

We thought that iPremier Company performed admirably as an organization during the 75-minute attack. Considering the early hour and lack of business continuity plan, the employees at iPremier responded as well as could be expected to the DDoS attack on the morning of January 12, 2009. In our review, we examined the individual performance of each employee, which helped us develop a comprehensive opinion about iPremier's performance during the attack.

In the IT department, we applauded Leon Ledbetter for his proactive response at the beginning of the attack. Despite the early hour, he informed Bob Turley of the problem with the company website and described to him the unusual messages received by support. He also quickly notified his manager, Joanne Ripley, about a possible attack, which was another wise decision. Alerting both Bob and Joanne, two more senior employees, meant the company could begin to marshal its resources to respond to the issue. Ultimately, his calls notified Bob of a potential attack and caused Joanne to decide to tackle the issue head-on at Qdata's data center.

Additionally, Joanne Ripley's quick response to the issue is worthy of praise. After learning about the possible attack from Leon, she called Qdata to ask them about the issue. When she received an inadequate response from Qdata, she immediately decided to go to their data center herself. At the facility, she had to go through additional bureaucratic hoops to gain access to Qdata's operations center. While her actions did not actually stop the DDoS attack, she gave it her best effort despite the number of obstacles. Overall, Joanne's dogged attempts to remediate the issue reflected well upon her.

Although Bob's conversation with Tim Mandel was brief, Tim did advise Bob to not physically shutdown iPremier's system, which turned out to be the correct response. When Bob asked Tim about unplugging the system, Tim immediately raised the issue of public disclosure, recognizing that iPremier would have had to publicly disclose details of the attack. Tim also realized they would lose all their logging information if they unplugged the system. Although their logging system was inadequate, Tim thought that it could still contain useful information about the attack and that it could be used to prevent a future attack.

Several of the executives did little to help guide the company through the attack. Warren Spangler, iPremier's public relations executive, unhelpfully speculated about what the attack might mean for the company's stock price. He also pledged to manage the PR for Bob Turley, which was not an area of concern at the time. iPremier's lawyer, Peter Stewart, seemed to be most concerned with making sure he would not be blamed for any potential fallout from the attack. CEO Jack Samuelson was able to assist Joanne with gaining access to Qdata's facility, but there was little he could do during the attack.

In our opinion, Bob Turley managed the situation well. After being woken up at 4:30 A.M., Bob did his best to grasp the situation and to consult subject matter experts within iPremier. His calls with Joanne were fruitful, and he provided her with clear guidance about how to proceed. It was also wise of him to consult

Tim Mandel, another of his IT managers, to get his opinion on the situation. We believe Bob did an excellent job filtering out the useless advice he received from Warren Spangler and Peter Stewart. During the attack, it was wise of Bob to spend as little as time as possible on the phone with his non-IT staff.

While we approved of Bob's performance overall, we identified steps he should have taken that would have improved his organization's response to the attack. We think Bob should have held a conference call with his technical staff to consult their opinions and to craft a unified response to the attack. Additionally, we thought Bob needed to identify and prioritize critical services and applications that held PII data. Prioritizing the security of PII data would have helped mitigate the damage from the attack and allowed iPremier to resume normal business practices more quickly. And finally, in our opinion, Bob should have documented all his actions during the attack. Had Bob taken detailed notes, he could have used his notes to identify areas of concern and to develop a better response plan for future events.

Key Question 2

The iPremier Company CEO, Jack Samuelson, had already expressed to Bob Turley his concern that the company might eventually suffer from a "deficit in operating procedures." Were the company's operating procedures deficient in responding to this attack? What additional procedures might have been in place to better handle the attack?

After reviewing the case study, we can confidently say that iPremier's operating procedures were deficient on many levels. CEO Jack Samuelson was correct when he stated that the company would suffer due to deficient operating procedures. To begin with, iPremier had a poor chain of command. For example, when the issue arose, the IT personnel Leon Ledbetter, who was on his nightshift duty, directly called the CIO of the company without having a clear understanding of the issue himself.

The case also shows that the company had an outdated emergency procedure plan. In one of his conversations with Joanne, Bob learns that the binder that has procedures to carry out in case of any technical emergency is out of date. The procedures do not apply to the technology they have been using, and the procedures have not been tested and updated. Because of this reason, most of the IT staff had no idea about how to go about fixing the issue.

Additionally, iPremier did not escalate the issue with Qdata until it was too late. Though iPremier had outsourced their data centers to Qdata and paid them for 24/7 support, iPremier did not receive any support on the day of the attack. It was clear that nobody was monitoring the network, as the person responsible was on vacation. We believe that iPremier should have had a better knowledge of how their assets were being managed at Qdata. They should have had contact details of managers and members of the team that were responsible for providing iPremier 24/7 support.

Physical access control at Qdata also turned out to be an issue since iPremier's IT manager was not allowed to enter the Qdata premises. Having to have the company's CEO make calls so that an IT manager could be allowed to access their own resources is embarrassing. iPremier should have established access control plans with Qdata, specifying how and who can access resources related to iPremier. Also, it would be important to establish role-based access control company wide.

We can conclude from most of the conversations Bob had with his employees that they did not know what their critical services and applications were. They were unsure if the attack meant that their PII data was accessed. Even after the attack ended, they were not sure if they had a data breach.

Bob Turley did his best to call all the key staff in IT and to try to understand the issue and to get their opinion on it. Additional approaches that might have helped would be to hold a conference call with IT team, legal team, and senior management of the company so that everyone could talk in one forum and conclude or produce a set of tasks that they will use to better manage the issue. Since he was constantly on the phone, Bob could not make a concrete decision on the nature of the attack and how to fix it.

iPremier should check the configuration and system logs. This will help them to investigate the issue and any unusual activity. Adding extra disk space to have detailed logging is critical as well. The company did not prioritize this as it would cut profits.

A few of the other things that the company could have done are inform law enforcement agencies, contact their ISP, and configure and set a "temporarily unavailable" webpage. This would be beneficial in case the attack lasted longer. It would be advantageous for iPremier to document every action taken during the attack. Documentation will help iPremier analyze where they went wrong and determine what they could do the next they experience an attack.

Key Question 3

Now that the attack has ended, what can the iPremier Company do to prepare for another such attack?

After the attack, we believe that iPremier has a lot of work to do and that change is necessary. Based on the known evidence, we cannot conclude that there was an intrusion, but we are certain iPremier experienced a DDos attack, which can possibly happen again soon.

We think iPremier should be concerned about their chain of command, service provider Qdata, operational plans, disaster recovery, backups, and business continuity plans. They also need to prioritize better security practices.

We recommend they implement the following solutions immediately:

1. Hire experienced security professionals and a create a Disaster Management Team. They should also create an Incident Management Team.

2. Security protocols should be introduced, and systems and devices should be updated on a regular basis inside the organization. A strong password policy needs to be mandated.

3. Need to have security and compliance training mandated for all the people (including the management) inside the organization and to introduce Roles-Based Access Control (RBAC) for all users.

4. They should immediately upgrade to a better service provider and make sure that their data is backed up, monitored, audited, pen-tested and analyzed regularly.

5. Ensure they are protected against data leakage, corporate espionage, and sabotage of sensitive information.

Additionally, the newly formed response teams must practice crisis management to ensure that they understand what do in the event of an attack. We also believe iPremier should mandate cybersecurity training for all employees, including executives. Most importantly, they need to conduct a thorough investigation of the incident.

Key Question 4

In the aftermath of the attack, what would you be worried about? What actions would you recommend?

After the attack, we would be most concerned about customer PII data that might have been accessed or stolen by the attackers. Since iPremier relies on online credit card transactions for payment processing, it is imperative that any stored information about their customers be secure. If the attackers managed to access any of this information, iPremier could be exposed to customer lawsuits and regulatory action from the government. Additionally, they could lose customers because of a breach, which would hurt their profits, stock price, and overall company reputation. Since iPremier is only barely profitable, any dip in profits because of a breach would be devastating to the company's bottom line.

The possibility of additional attacks was another area of concern. While company personnel responded quickly to the issue, the attack ended on its own after seventy-five minutes, which was fortunate for iPremier. We thought that iPremier might not be as lucky the next time they were attacked. Since the DDoS attack could only be the start of a campaign against iPremier, we would be extremely worried about subsequent attacks.

In addition to the possibility of other attacks, iPremier must understand the extent of the attack that they experienced in January 2009. After the DDos attack mysteriously stopped, Bob and Joanne debated whether the attack was the work of unsophisticated attacker (script kiddies), or if the attack was complex in nature. Not only must Bob and Joanne understand the complexity of attack, but they must also determine if there was an intrusion into their internal systems.

To address these concerns, we believe iPremier should conduct an internal audit of the attack, in addition to hiring external auditors. iPremier must understand why the DDoS attack was successful and ensure that there was not also an intrusion. They must make sure their internal systems are secure and that the attackers are not lurking on their network. External auditors should assist iPremier with this, as iPremier's technical capabilities are rather limited. Hiring external auditors will demonstrate to their customers and investors that they take the DDoS attack seriously and that they are taking the appropriate steps to protect sensitive data.

iPremier must be better prepared to deal with an attack in the future. The company needs to develop a business continuity plan and a detailed list of emergency procedures. Company personnel should be knowledgeable about this plan and routinely practice dealing with an attack. In our opinion, iPremier needs to reevaluate their relationship with Qdata. During the attack, Qdata personnel appeared incompetent and were unhelpful in resolving the issue. iPremier must decide if they want to continue this relationship, or if they should hire another service provider, or develop their own internal IT systems. Regardless of their choice, iPremier's relationship with Qdata must change for the better.

Risk Assessment

Risk assessment is the process of assessing the relative risk for each vulnerability. Our team performed a risk assessment based on the information provided in the case study. We identified the assets, vulnerabilities, threats, and controls. Due to the issues we identified with Qdata and their weak firewall, iPremier has a high chance of DDoS attack. iPremier also deals with PII data of customers, which makes it prone to ransomware attacks. Other threats include malware and insider threat. These cyberattacks can result in intrusion and data breach.

In order to prevent these attacks or mitigate the impact of these attacks, iPremier should upgrade their firewall, improve Qdata or shift to another IT service provider, have a record of logging details, and come up with a better business continuity plan. Refer the exhibit for a detailed analysis.

Our Solution

iPremier needs a better chain of command that increases efficiency, supports everyone within the organization, simplifies delegation, creates accountability and clarity, and most importantly, standardizes communications. Additionally, iPremier should create a crisis management team and have incident management plans.

We recommend that iPremier replace Qdata with a new service provider. Hiring a new service provider will increase customer trust, increase business reliability, and reduce the risk of future attacks. Their new service provide must ensure that they back up monitor iPremier’s data.

We believe that iPremier should hire experienced IT and security professionals. The newly hired security professionals should establish and mandate safety protocols. Also, iPremier must update their systems and devices on a regular basis. The company must follow best practices by enforcing a strong password policy, requiring unique passwords that are difficult to crack for each employee. In our opinion, iPremier should establish role-based access controls for all members of their organization. Role-based access controls will improve efficiency, ensure compliance, and help prevent security incidents. They must also conduct an enterprise-wide risk assessment, developing a clear understanding of the organization’s risk and establishing policies and controls to combat this risk.

Finally, we believe iPremier needs security and compliance training which will increase resilience to phishing attacks, help alleviate security costs, reduces the risk of insider threats, and create a strong security-minded culture. Employees must think and act with a greater awareness of security.

Conclusion

iPremier’s official values were discipline, professionalism, and partnership for achieving profits. We believe iPremier’s management prioritized making profits over improving their IT infrastructure. This is the why they continued to outsource the company’s IT services to Qdata even when they knew Qdata’s services were lacking. The DDoS incident occurred three months after Bob’s onboarding at iPremier, and he also did not talk about moving to a different provider.

Though iPremier paid Qdata for 24/7 support they were not of any help during the attack. On further enquiry, iPremier found out that the Qdata employee who was responsible for monitoring network traffic was on vacation. Qdata did not put anyone in charge during the time the support person went on a vacation. This clearly shows that Qdata’s management was incompetent and continuing to be outsourced to them or even paying them for 24/7 support was not a good idea.

In their conversation during Bob’s onboarding, Joanne tells Bob why iPremier continues to use Qdata. One of major reasons was that one of the iPremier’s founders knew Qdata’s founder. Companies should IT choices based on technology and how competent the company. Failure to do this will most probably result in incidents like the one they just experienced.

Leon, the IT guy, mentions to Bob that the staff in IT are playing online video games, which shows that the IT staff is misusing company resources. This signifies that there was no resource usage policy and none of the managers took any actions against staff paying games online. All these points show that iPremier did not prioritize IT, and they made no effort to make security stronger. Therefore no one had a clear picture of the nature of the attack and how it affected the internal systems at iPremier.

Most importantly, iPremier did not have a complete understanding of the nature of the attack, instead they were forced to be just reactive to stop the attack. Bob never knew what exactly was happening, and he was never able to decide about the correct course of action. Although a few of the iPremier employees were proactive, not everyone was working in the right direction as they were not prepared for such attacks.

Exhibit

Assets

- PII data - like SSN, credit card information, etc.
- Internal IT infrastructure - Web servers, routers, switches, firewall
- Company reputation
- Customer trust
- Stock value

Vulnerabilities

- Qdata
- Out-of-date business continuity plan
- Inexperienced team and Incompetent management
- Weak firewall
- No proper line of control

Threats

- DDoS – targeting router
- Malware
- Ransomware
- Insider Threat

Controls

- Upgrading firewall
- 24/7 monitoring
- Upgrade server capacity – make sure company has record of logging details
- Access control at Qdata - Joanne Ripley, IT manager, should have access at Qdata
- Better business continuity and disaster recovery plan
- Information security and cybersecurity awareness training - compliance
- Conduct internal audit and regular audits – hire external auditors

Threats	Probability (0-100%)	Impact (1-5)	Risk Rank	Decision
DDOS	85%	5	1	Risk Mitigation/Transfer
Ransomware	70%	4	2	Risk Transfer
Malware	40%	3	3	Risk Transfer
Insider Threat	20%	2	4	Risk Mitigation

Figure 1: Quantitative Risk Analysis

Threats	Probability (0-100%)	Impact (1-5)	Risk Rank	Decision
DDOS	Very High	Very High	1	Risk Mitigation/Transfer
Ransomware	High	High	2	Risk Transfer
Malware	Medium	Medium	3	Risk Transfer
Insider Threat	Low	Low	4	Risk Mitigation

Figure 2: Qualitative Risk Analysis

References

https://www.mpug.com/understanding-qualitative-risk-analysis/

https://nanopdf.com/download/how-did-ipremier-perform_pdf

https://www.termpaperwarehouse.com/essay-on/The-Ipremier-Company-a-Denial-Of/210551

https://youtu.be/2zpLWsYu9RA