Scott Hirabayashi

ENMG 652

**“IPremier (A): Denial of Service Attack” Case Study II**

**Executive Summary**

Bob Turley has taken a new role as Chief Information Officer (CIO) at iPremier, a company with a Business to Consumer (B2C) model that caters to a high-end clientele. Jack Samuelson, the head of iPremier, has tasked Bob with moving iPremier forward into the future, a significant task, as iPremier has a history of mixed success. Since its inception, iPremier has gone through the early excitement and subsequent plummet during the internet stock boom and crash. Presently, iPremier has reached limited profitability through an “intense” business culture, which values timeliness and delivery.

However, Bob and his staff also note several significant weaknesses within iPremier’s technological infrastructure, organizational communication, and business partnerships. These challenges are exacerbated when three months into Bob’s tenure with iPremier, the company experiences a sophisticated denial of service (DoS) attack aimed at the company’s routers. The immediate urgency of dealing with the issue raises the attention of the full executive team, and the IT team. In communication with his IT department head, Joanne Ripley, as well as the executive team, Bob ‘solves’ the issue of the DoS attack, as the attack unexpectedly eventually stops.

Bob and his team are left unsure of its effects, particularly, the possibility of stolen customer credit card data. Through the ordeal, iPremier’s significant systemic flaws are made evident: specifically, lack of communication, planning, and knowledge on the part of the team.To effectively move into the future, Bob and the executive team will be tasked with making the necessary technological and cultural changes needed to protect from future attacks.

**Challenges**

Lack of emergency procedures plan: Leon Ledbetter, the software engineer on-site who first alerts Bob, is unsure of what to do when the DoS attack begins. He also reports that he is unsure of the existence and placement of the binder that outlines iPremier’s emergency procedures for an internet attack. Joanne Turley, who manages Leon’s team, shares that there is a resource for emergency procedures, but that they are out-of-date, making them useless throughout the attack. Without an updated set of business continuity plans, the iPremier site is rendered unusable, and has led to complaints to the company’s help desk, meaning both lost sales, and lost trust.

Additionally, while the lack of training for this particular DoS attack is concerning, the lack of generalized procedures for iPremier is far worse. It endangers the future of the company; as it essentially means there are no emergency procedures for an attack on iPremier. *Any* successful attack on iPremier would be met with the same effect: lost business, lost consumer trust, and perhaps, lost customer data. And, if Leon’s lack of knowledge serves as an example, iPremier has functioned for a significant period without planning or training for them.

Lack of knowledge about the actual attack: As the attack on iPremier progressed, Bob saw increasing issues about iPremier’s understanding of the DoS attack itself. Was it just a DoS attack, or was there an intrusion on iPremier’s systems? Were credit cards and information stolen? As the attack goes on, there is a shared lack of understanding for what is being targeted, what may be stolen, and what risks are being placed on customer data. Upon the fortuitous and unexpected conclusion of the attack, Bob and Joanne are left to consider these questions, and the fallout from the attack itself. Even this step will be difficult- Bob learns that there is little data storage currently being allotted to logging data throughout attacks on iPremier.

Issues with organizational communication:Bob’s initial exposure to his team and the company hints at the communicative issues between iPremier’s departments. The IT department is referred to as the “dungeon”, secluded from the rest of the company, and on a different floor from other company operations. Moreover, iPremier’s isolated IT department is also far removed from their data center, which is controlled by Qdata and offsite. When Bob finds himself confronted with the DoS attack, he is on a business trip to New York, and struggles to effectively guide his team.

Bob is forced to coordinate with his subordinates and the executive team by phone. Immediately, we see the scale of this challenge: while Bob, Joanne, and Leon reach out to the central employees within iPremier, the executives and managers struggle to raise their competing interests and concerns about the attack within the company. At times, Bob is unsure of the information that has been provided to the important members of iPremier about the attack.

Last, as iPremier’s data operations use a third-party data center (Qdata, a contracted service), communicating the problem and attack with them is similarly made difficult through a lack of communication with the data center. As soon as the attack happens, Joanne quickly travels to the nearby Qdata site, but is restricted from access. She is unable to immediately access Qdata’s datacenter to diagnose the problem, losing valuable time and information about the nature of the attack. It is only when Bob requests that Jack Samuelson, who heads the company, to contact Qdata, that Joanne is able to troubleshoot the attack with Qdata’s on-site staff.

**Root Cause**

Misplaced emphasis on company performance and growth: iPremier is based on a business-to-consumer (B2C) model. They generate “high-end” sales on many expensive products, thus heavy emphasis should be placed on their customers. However, upon numerous occasions iPremier demonstrates their overemphasis to instead produce and grow, and ignore or overlook other important aspects of the business. Mainly, they have cut costs and overlooked key needs within their business in the interest of improving competitiveness and profitability.

The official iPremier company ethos is “discipline, professionalism, and partnership for achieving profits” (Austin & Short, 2019). It contains no language about valuing customers or promoting a positive work culture that values its employees, nor for valuing the customer. Bob learns that unsuccessful managers are quickly removed from their posts, and that their original employees are being replaced by “experienced managers'', likely those who are external to the company. Within iPremier, the organization appears to be low trust, further exacerbated by the separation of departments and business operations within the company itself.

Moreover, a central issue for iPremier throughout the attack is iPremier’s lack of thought and preparation. Joanne and Leon share little knowledge of the attack, and Bob, responsible for the department, also brings no understanding of the business continuity and emergency plans that could have saved iPremier from the numerous communication issues that arise. Bob discovers that, in fact, there is no current and central plan for dealing with an attack. Until there *is* a current plan in place, and employees and executives are trained in the procedures of the attack, these panic scenarios will continue to happen.

For data storage, iPremier only holds limited logs of data; one manager notes that detailed logging is not enabled, which will lead iPremier to struggle to understand and recreate the nature of the attack. It appears that iPremier has not had a similar attack to this point, but there are no guarantees their good luck will continue.

Qdata is another strong example of cost savings that end up being dangerous for iPremier. Qdata, the contracted data center for iPremier, provides space, power, and communications. Using Qdata serves as a cheaper alternative over building their own facilities, and there is also a connection between the founders of both companies. However, Qdata does not appear able to fill the iPremier’s needs, and it appears to be breaching its contract with iPremier.

The IT team at iPremier does not speak highly of their services, and during the attack on iPremier, the dangers of contracting with their organization are shown in-full. First, despite there being a contractual obligation for 24/7 support, Joanne is initially unable to access the facilities or receive support. She is also informed that there is no one on-site to assist or allow her to access the facilities, and it takes Samuelson’s intervention to allow her to understand the basics of the attack. Second, Joanne notes that Qdata’s firewall protection itself is poor, meaning that Qdata and iPremier are vulnerable to future attacks as well. Clearly, iPremier is currently not up to the task of protecting iPremier’s data.

**Recommendations**

Bob is left with many options as to how to proceed with shoring up iPremier’s policies to protect against future issues. A description of the recommendations for Bob and iPremier are as follows:

* Amend company values/ethos to include focus on customers and employees: The values of a company are important. Steinhorst (2019) writes “ Core values have weight, especially when they’re truthful and focused on what matters to the community within the organization.”For iPremier, their company values’ lack of emphasis on valuing their employees and customers over other business responsibilities. In building employee *and* customer trust, iPremier can ensure future events by proposing a revision of their original values and ethos, so as to take actionable future steps that move emphasis to customers and employees- areas that should be valued.

Steinhorst says that a company’s understanding of their values can unify its employees to a common mission statement. He warns however, that a company’s values must be authentic, “Values are an investment, not a platitude”, he writes, suggesting that iPremier will have to carefully consider what they are, and what they should aspire to be to improve customer and employee relationships.

* Create an emergency plan:This could be the first time that iPremier has experienced an online attack, but it will certainly not be the last. Cybercrime is on the rise, and iPremier will need increased protection from cybercrime moving towards the future. Morgan (2018) states that cybercrime may grow up to $10.5 trillion by 2025, and is projected to increase by 15% each year. He writes “This represents the greatest transfer of economic wealth in history”. iPremier’s status as a small business would not exempt them from attacks either, Morgan writes that “More than half of all cyberattacks are committed against small-to-midsized *(sic)* businesses (SMBs), and 60 percent of them go out of business within six months of falling victim to a data breach or hack.”

Erlanger (2006) suggests that this process be decided by first drafting business needs, and utilizing a framework such as COSO (Committee of Sponsoring Organizations of the Treadway Commission), or COBIT (Control Objectives for Information and related Technology), which are designed for drafting business continuity plans. Erlanger suggests that companies should begin with a business impact analysis, so that they can focus on dependencies and needs in the event that a business can function in the case of attacks or emergencies.

* Consider Alternatives to Qdata: Qdata’s lack of support and immediate access to their data center lost iPremier valuable time and ability to decide on how to proceed. While Qdata may have been experiencing a rare event of operational and technical difficulties, iPremier should scrutinize the failures of the event, hear Qdata executives speak on improvements they will make to their own operations, and also consider possible alternatives, such as building a data center on-site, or contracting with an organization that may be more expensive, but would not have caused the same issues.

Sears (2020) outlines ten primary considerations for deciding on a data center:

colocation, location, connectivity, tier classification, reach, security, backup and disaster recovery, access and maintenance flexibility, green credentials, and price/value. Of this list, the recent online attack shows significant weaknesses in security, backup and recovery, and access and maintenance flexibility. If iPremier wishes to remain competitive, they require a thorough examination of the weak points in their company. Qdata is one of them, and unless iPremier can be confident that Qdata can improve honor and improve the services they provide, iPremier should look elsewhere.

**Recommendation Table**

| **Recommendation** | **Rationale** | **Description/Time Frame** | **Criteria for Success** |
| --- | --- | --- | --- |
| **1. Amend company values to include focus on customers and employees.** | The company’s emphasis on growth and profitability has had a negative impact on employees and customers.  By redefining the stated company values, iPremier could take its first steps towards a healthier and more-holistic business model. | * (Immediately) Executive team meets and discusses initial ideas about each department’s intended direction for iPremier, and the most important company values for success. * (Within the first month)Executives work to draft a set of 3-5 company values that incorporate a focus on their employees and their customers, to better reflect a changed focus. These should be incorporated into a revised company charter. * (2 weeks after draft) Executives decide on a distribution method to inform their employees and customers about their revised focus. * (1 week after distribution decision) Afterwards, employees and customers are both contacted on iPremier’s revised aims and values. * (Within two weeks of the new charter sent) Employees read, ask questions, and sign off on the new charter and values. They are also asked to submit ideas for actionable ways to improve company culture (internally and externally). | * Each iPremier employee has signed the revised charter and iPremier business aims. * Executive team solicits feedback on how to take actionable steps to improve relations between employees and customers. |
| **2. Create a Business Continuity Plan** | iPremier requires a way to maintain some business functions in the event that a future online attack or hack happens on their systems. | * (Immediately) Executive team is briefed on the nature and significance of the recent attack, and potential iPremier website vulnerabilities. * (Within the first 2 weeks) The Executive team discusses the nature of their business with a business impact analysis in the case of an internet attack. Subsequently, executives talk to each of their teams within iPremier to ensure that each department is represented. * (Two weeks after discussion) Executives use recommendations and draft the list of essential business requirements needed for ensuring iPremier’s most important parts remain online during attempted hacks/attacks, using the COSO or COBIT framework. * (Before two months) iPremier executives share the business continuity document with all departments, and resources and binders are created and accessible to any employee who may be affected by an internet hack. Executives and IT establish a schedule for updating information to ensure its relevance. * (Within two months after business continuity completion) The HR department works to establish training and seminars to share updated business continuity information with staff. | * iPremier has a plan in-place for any online attack. * Employees show an immediate understanding of the procedures for a hack, or will be immediately trained in the proper procedures. |
| **3. Consider alternatives to Qdata** | Qdata systems and services failed iPremier when they were needed.  Executives should give consideration to new alternatives. | * (Immediately) Hold a meeting with Qdata executives to understand why there are security weaknesses (no firewall, etc.) and access issues, and what improvements Qdata will propose to solve these issues. * (Within 1-2 weeks after meeting) Hold a meeting with executives, the IT team and other data stakeholders to gain feedback on Qdata services, and business and security needs that are not being met. * (1-2 weeks after 2nd meeting) Raise concerns to Qdata executives about additional problems with services. Inform them that iPremier is reconsidering their services and contract. * (within 1-2 months after 3rd meeting) Look externally for other data providers in the area, create a cost-benefit analysis chart between Qdata services and possible competitors. * (After competition of analysis) Vote and make a decision about the best data center option for iPremier moving forward. | * Discussion and debrief with Qdata held. * Shared reflection and revised expectations for Qdata team, and cost-benefit analysis by team completed. |

**Summary**

Early into his role at iPremier, Jack Samuelson tells Bob that he is hopeful that Bob can “take us to the next level” as an organization. While the fallout from the DoS attack is still fresh, Bob should advocate for several near and long term iPremier cultural changes that can improve their protection. With proper thought, foresight, and tweaks to the communication and culture within the organization, iPremier can set itself up for lasting success, preparedness for emergencies, and safety from future online attacks. However, without it, iPremier runs the great risk of prolonged security challenges, similar future issues, and liability from lost customer data.

**References**

Austin, R., & Short, J. (2009). iPremier (A): Denial of Service Attack (Graphic Novel Version). Harvard Business School.

Erlanger, L. (2006). In case of Emergency Activate Business Continuity Plan. InfoWorld, 28(32), 27–31.

Morgan, S. (2018, February 21). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>

Sears, S. (2020, May 17). *Top 10 considerations for selecting a data centre provider*. Technology Magazine. <https://technologymagazine.com/data-and-data-analytics/top-10-considerations-selecting-data-centre-provider>

Steinhorst, C. (2019, October 17). Rethinking the value of core values. Forbes. <https://www.forbes.com/sites/curtsteinhorst/2019/10/17/rethinking-the-value-of-core-values/>