MINICASE: Reinventravel.com Comes under Fire

As you watch the sun setting over the San Francisco skyline from your hotel room window, you can't avoid feeling that you really dropped the ball this time. You can still hear Clive Sturling, your chief information officer (CIO), as he tells you, "Don't worry about security. That's techie stuff; I'll take care of it. Just grow the business. That's what you are good at." You had not asked about security again after that conversation, perfectly happy to leave the "techie stuff" to him, and that was before you launched the company over two years ago!

Well, it was him on the phone a minute ago, ruining what had been a perfectly good day. In a daze, you replay the conversation in your mind: "We have been attacked," Clive had said. "It was a distributed denial of service attack (DDoS)— not much we could do with our current security infrastructure. The site was unavailable for about 70 minutes; it wasn't defaced or otherwise ruined, just down. I don't think many people noticed. The attack ended about an hour ago. I didn't want to call you before checking if they had compromised any files or stolen customers' data. It doesn't look like it."

Not much we could do? Isn't he the one who said not to worry about security? The site was down for "only 70 minutes." Does he know that in that amount of time reinventravel.com typically processed 19,000 transactions? Granted, evenings were a bit slower, but there must have been at least 4,500 customers who noted the outage. Your emotions kept mixing at a dizzying pace. You were angry at Clive; you trusted him, and he let you down. However, you felt sympathetic to his position as well. You had been the one who told him to "run IT on a shoestring," to help you speed the path to profitability as much as possible.

Oddly enough, as you begin to recover from the shock of the news, your college days flash into your mind, bringing a smile to your face. You had started in this field only three and a half years before, when you learned in one of your classes about the opportunity to revolutionize how people seek and purchase travel products. That day in your information systems class seemed like decades ago; now you were the chief executive officer (CEO) of a growing company with 52 employees, over 70,000 active customers and members, and revenues approaching $8 million. Clive had built the search engine in just eight months alone! He was a wizard with that kind of stuff. Half the time, you had no idea what he was doing, but as for the user interface, you certainly appreciated and understood that part of his work; everyone did! It was so far superior to anything that had been seen before . . . it was that fabulous demo that got you your first round of venture capital financing.

Financing . . . that word snapped you back to reality! You had to get ready for dinner. The meeting with your venture capital (VC) was in less than an hour, and you had yet to take a shower. With the first round of financing beginning to run out and minimal profits, a second round was a must. You had hoped to spend the evening discussing your plan for growing the customer base and beginning to monetize your membership, seeking their guidance and help with regard to the three potential partners you were evaluating. "Well, that ain't going to happen," you mumbled.

What should you do? Should you tell your VC about the denial-of-service attack? It may not be your choice; these guys liked to do their homework, and the odds were good that they were

poking around the site when the outage happened. No time to call your legal counsel; you had to go it alone on this one.

Clive had been very unclear about whether an intrusion had occurred along with the denial-of-service attack. At this point you had little faith with regard to his staff's ability to find out; it seems that security and monitoring had not been ranking very high on their priority list! reinventravel.com stored quite a bit of personal information about customers, including identifying information and credit card data. Should you communicate to the customers that an attack had occurred? Should you issue a press release? There was no evidence that security had been compromised and even less that personal data had been stolen. A denial-of-service attack only made a website unavailable for some time, did it not? "No way, Clive and his staff would know if data had been stolen," you told yourself.

This was increasingly looking like a situation you were ill prepared to address. But as your father always said, "You wanted the bicycle? Now you have to pedal." As you began to feel the adrenaline pumping again, you exclaimed, "Here we go!" and jumped up from your chair. You had 55 minutes to develop your plan before dinner.

Discussion Questions

1. Do you agree with the assessment that you had dropped the ball? Or are you being unduly harsh on yourself?

2. Who do you think should be making security calls at Reinventravel.com? Shouldn't this be the CIO's job?

3. What should you do tonight? Should you approach the topic at dinner or wait and see if anyone else raises the issue?

4. What should you do in the next few days? Should you issue a press release? Should you contact your customers directly? Should you focus on overhauling your security safeguards to prevent future similar problems and forget today's incident?