HARVARD | BUSINESS | SCHOOL

9-601-116

REV: FEBRUARY 28, 2018

ROBERT D. AUSTIN

The iPremier Company (C): Distributed Denial of Service Attack

The iPremier Company's senior management decided not to shut down the business for a comprehensive rebuild of all production platforms. Using whatever equipment they could scrounge from other uses (to reduce cost and impact on profits), they *did* embark upon an accelerated plan to create an iPremier site in a more up-to-date hosting facility.

Two weeks later, on January 26, a call from FBI Special Agent Donald Reedy in Washington, D.C., was routed to Bob Turley's desk. Reedy informed Turley that for the past two hours the iPremier Company's biggest competitor, MarketTop, had been experiencing a distributed denial of service attack. The source of the attack, Reedy explained, was inside iPremier's production computing installation.

The iPremier operations staff quickly located and killed computer processes that were the sources of the attack. A file that had spawned some of the processes resided on a database server. This proved that the firewall had been penetrated. Computer security experts whom Ripley and Mandel consulted speculated that the January 12 distributed denial of service attack against iPremier might have been a misdirection tactic, to divert attention from hacking. This sort of "suppressing fire during retreat" was a common tactic used by sophisticated hackers, according to these experts.

The senior team now faced three difficult issues.

The first was familiar: whether to immediately implement Ripley's rebuild recommendation. Some still resisted this idea, arguing that the MarketTop attack might be the full extent of the nastiness the intruders had intended and that the other site would be up soon (although it was now looking more like four to six weeks to get it up and running). Moreover, Legal Counsel Peter Stewart pointed out that the issue was now more complicated. Since iPremier computers had been the source of an illegal attack, the FBI might well consider a rebuild to be destruction of evidence of a crime.

The second issue was also legal in nature: how to handle the situation between iPremier and competitor MarketTop. Stewart suggested that MarketTop could probably mount a lawsuit against iPremier for its apparent role in the January 26 attack. It was not certain that they would do it, though,

---

Professor Robert D. Austin, Dr. Larry Leibrock (Chief Technology Officer, McCombs School of Business, University of Texas at Austin), and Alan Murray (Chief Scientist, Novell Service Provider Network) prepared this case. This revised version was prepared by HBS Emeritus Professor Richard L. Nolan, Professor Robert D. Austin (Ivey Business School), and Professor Michael Parent (Beedie School of Business, Simon Fraser University). HBS cases are developed solely as the basis for class discussion. Cases are not intended to serve as endorsements, sources of primary data, or illustrations of effective or ineffective management. The situation described in this case is based on real accounts of denial of service attacks directed against several companies during 2000 and 2001. Company names, product/service offerings, and the names of all individuals in the case are fictional, however. Any resemblance to actual companies, offerings, or individuals is accidental.

because the suit would become public and bring attention to both companies that neither wanted. There was no agreement on whether or how to approach MarketTop.

The third issue was also familiar: What to say publicly. The database server that had been compromised contained credit card numbers. This meant that someone *could have* stolen credit card numbers. But it did not prove that anyone had *actually* stolen credit card numbers. iPremier could not identify individual customers who had been affected. The issue that was discussed heatedly by the senior team was what the company should disclose publicly. Stewart also suggested that iPremier could be in violation of its credit card processing agreement covenants, and if so, lose the ability to process credit card payments.

Turley argued in favor of disclosing what might have happened. Linda Kliewer, iPremier's Chief Financial Officer (CFO), offered a different view:

> "Suppose someone broke into our offices and I'd left some customer information in one of my unlocked desk drawers. Sure, they could have gone into my desk and made copies. But did they? There are many things pranksters might have done. Suppose my desk drawer is just as I left it, to the best of my ability to confirm. I don't have any evidence that they actually did go into my desk. In a case like that, would we go public to say that it is within the realm of possibility that the burglars took some customer information?"