HARVARD | BUSINESS | SCHOOL

9-601-115

REV: FEBRUARY 28, 2018

ROBERT D. AUSTIN

# The iPremier Company (B): Distributed Denial of Service Attack

A few hours after the attack, iPremier disclosed publicly that it had been the victim of a distributed denial of service attack. A company spokesperson emphasized that the event had lasted only 75 minutes during the middle of night, and that only a few customers had been inconvenienced. Nevertheless, the company stated that it would revisit its already solid computer-security measures. The stock price was not discernibly affected and the event was not a major topic at that afternoon's analyst meeting.

After the attack, the company instituted new security measures, which are listed in **Exhibit 1**. The company was not, however, able to determine whether the firewall had been penetrated. There was no conclusive evidence that intruders had succeeded in tampering with the company's production computer equipment. But there was no conclusive evidence that intruders had *not* compromised the firewall, either. Every file on every production computer was examined for identity and size, but the company's "fingerprint" that told which files should be on production machines had not been kept up-to-date. So there was no guarantee that the file-by-file check of every file would detect, for example, a file that had been replaced by an altered file of the same name.

It was this uncertainty about what had actually happened that led Joanne Ripley to offer a refined recommendation that some still regarded as extreme: disconnect all production computers from the Internet and rebuild the software systems on all of them from development files (which were presumed much less likely to have been tampered with, if there had been intruders). Operations staff estimated that the company would need to completely shut down its business for 24 to 36 hours to complete such a comprehensive rebuild. Although the rebuild processes were theoretically well-documented, some people in operations were concerned that there might be hiccups during the rebuilds that could delay getting everything back online.

Whether to implement Ripley's recommendation was the subject of heated debate among senior managers. Ripley stuck to her guns, noting that the attack had been quite a bit more sophisticated than a routine DDoS attack and that a complete rebuild was "the only way to be sure." Warren Spangler vehemently opposed the plan. "It would be irresponsible of us to take such action," he argued, "knowing that it was certain to significantly degrade customer satisfaction at a time when we are trying

---

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.

to maintain sales and profit growth in the face of fierce competition." He pointed out that iPremier's situation was pretty much the same as it had been before the attack. Neither before nor after the attack was there evidence that production equipment had been compromised.

Resistance to Ripley's plan led to discussion of another option: They could build a new site in a new facility from development files, then switch the old site off only after the new site was up and running. The company would not have to be shut down and the new site would (probably) be free of any nasty surprises that an intruder might have introduced. This accomplished, argued some, the same thing as Ripley's recommendation, without disruption to the business.

It would, however, be costly to obtain space in a hosting facility and new equipment for a new site. Also, if the production equipment and files had indeed been compromised, keeping the old system live could exacerbate any negative situation. The time it took to create the new site was time when further nastiness might materialize from intruders – if there had been intruders.

"Bad things can happen in three weeks," said Ripley.

**Exhibit 1** Security Measures Instituted by the iPremier Company Following January 2018 Attack

- Restarted all production computer equipment (not at the same time—no customer interruptions).
- Conducted a file-by-file examination of every file on every production computer to look for evidence of files or parts of files that should not be present.
- Began a study of technology solutions that might be used to assure that files on production computers were the same files initially installed there.
- Expedited a project aimed at moving to a more modern hosting facility.
- Modernized computing infrastructure to include a more sophisticated firewall.
- Bought additional disk space and enabled high levels of logging so there would be more diagnostic information available after any future attacks.
- Trained more staff in the use of monitoring software; educated all about security threats.
- Created an incident-response team and practiced a simulated attack.
- Began an executive search for a Chief Security Officer.
- Retained a cybersecurity consulting firm.
- Instituted monthly third-party security audits.

Source: Casewriter.