Crisis

When Disaster Strikes IT

Excerpted from

The Adventures of an IT Leader

By

Robert D. Austin, Richard L. Nolan, and Shannon O'Donnell

Buy the book:
Amazon
Barnes & Noble
HarvardBusiness.org

Harvard Business Press
Boston, Massachusetts

ISBN-13: 978-1-4221-3042-1
3024BC

SERIES OVERVIEW

The Adventures of an IT Leader invites readers to "walk in the shoes" of a new CIO as he spends a difficult year learning effective information technology leadership. Experienced cumulatively, this eighteen-chapter story gains dramatic momentum, and later chapters provide opportunities to revisit key IT management issues in more depth. However, chapters can also be read independently or in smaller batches as suits the needs of particular readers. To facilitate this, we provide the following contextual information.

SUMMARY

As the story begins in chapter 1, the IVK Corporation, a midsize financial services firm, is attempting a turnaround following a period of slowing business performance[1]. The stock price has fallen substantially as investors have adjusted their expectations of the firm's growth. An aggressive new CEO, Carl Williams, takes over and assigns a new management team. In the process, the former head of Loan Operations, Jim Barton, is appointed CIO. Barton has no background in IT—none at all. The story

[1] The IVK Corporation and its staff are fictional, but the contents of the book are based on the authors' years of firsthand experience with diverse companies and managers.

follows Barton as he figures out what effective IT management is all about and deals with issues and challenges of the job. These broadly include, by chapter number:

- The challenges of information technology leadership (1–3)
- Managing the IT budget (4)
- Maximizing the value of IT (5)
- Approaches to project management (6)
- Managing large projects (7)
- Prioritizing among a portfolio of projects (8)
- Board-level governance (9)
- Management and aftermath of a security crisis (10–11)
- Communication and interaction with the boss and peers (12)
- Analyzing emerging technologies (13)
- Arranging and managing partnerships with vendors (14)
- Managing highly talented employees (15)
- Investing in infrastructure to move toward standardization and innovation (16)
- Managing risk (17)
- Job opportunities for IT leaders (18)

The Main Characters

In order of appearance . . .

Jim Barton: The new CIO of IVK. A talented and ambitious general manager, formerly the head of Loan Operations. Barton knows little about IT; he sets out to learn quickly and to lead the IT department toward renewed growth, stability, and strategic partnership within the company—but not without facing serious challenges.

Carl Williams: This bold turnaround CEO is high on ambition and short on patience.

Maggie Landis: A savvy management consultant and Barton's girlfriend, she often provides Barton with valuable insight, references, and perspectives.

The kid: Wise beyond his years, this twenty-something tech nerd, whom Barton mysteriously meets only at Vinnie's Bar, proves a useful sounding board and source of surprisingly good advice.

Bill Davies: Former CIO at IVK, Davies was fired in part because he struggled with management-level communication. He tells Barton that he "won't last one year" in the job of CIO.

Bernie Ruben: As the director of the Technical Services Group and longtime IVK employee, Ruben is nearing retirement and thus mostly immune to concerns about risk to his career. He frequently provides Barton with the candid advice, knowledge, and context he needs to make key decisions.

Raj Juvvani: The director of Customer Support and Collection Systems and part of Barton's core IT team.

Tyra Gordon: As director of Loan Operations and New Application Development Systems, Tyra worked closely with Barton when he was head of Loan Operations and takes the lead on several new IT projects under his management.

Paul Fenton: Director of Infrastructure and Operations, Fenton manages a large and important domain, including IT security, and is part of Barton's core IT team.

Gary Geisler: As director of Planning and Control, Geisler works closely with Barton on IT financials.

John Cho: IVK's outspoken resident security genius, Cho has a distinct fashion sense and provocative musical talent.

Jenny: Barton's ever-dependable executive assistant.

Several additional characters populate the story, but are described in context.

CHAPTER TEN

CRISIS

Thursday, June 28, 9:24 a.m. . . .

Barton was enjoying an unusually slow morning, finishing an elegant breakfast at a Hilton in midtown Manhattan, when the first call indicating trouble came in.

He had come to New York for an early afternoon meeting with Wall Street analysts. That Williams had chosen him for the meeting was a sign of just how well things had been going lately for IVK—and for Jim Barton, CIO. In the past three weeks, IVK's stock price had begun to rise, lifting spirits throughout the company. Optimism percolated through the offices and hallways. At the same time, Barton had been scoring victory after victory. A recent all-hands IT department meeting had gone extremely well; he'd fielded a few tough questions, but people seemed pleased with his answers and the department's overall direction. Even John Cho had nodded in response to some of Barton's remarks. His resolute actions had also gained him the confidence of the company's senior leadership. In meetings of that group, Barton's views now swayed Williams more readily than anyone else's. And why not? This was a guy who knew the IVK business inside and out and had apparently mastered the mysterious world of IT in just three months.

Sending Barton—former Loan Ops VP, now chief IT guy—to New York on the crest of a wave of recovery, Williams had explained, sent exactly the right message. Under a new CEO, IVK had woken up to a

realization of its current size and the consequent need for a new style of management. The company would *mature* into a grownup financial services firm. What had been a freewheeling, improvisational approach to management would become more professional. Without sacrificing organizational agility, the company would institute more formal systems and controls. IT was, of course, key to achieving this. An expression Williams and Barton had begun to use in conversation to describe where they were headed captured their joint vision of the future: "a lean service factory." It was only natural that Barton would explain all this to Wall Street.

He'd been sipping coffee, going over his notes, making some last-minute adjustments to the presentation for the afternoon meeting, when his cell phone rang. The phone display told him it was Bernie Ruben. Barton guessed that the call might be last-minute advice about how to tweak the analyst presentation.

He was wrong.

"Hi Bernie, what's up?"

"Hi Jim. I'm afraid we've got a problem, and we felt we should get to you with an update."

"My laptop is upstairs. Is it something I need to change in the presentation?"

"Nothing like that. We're experiencing an outage this morning, for about the last forty minutes. Customer Service is down. None of the call center systems are working, and the Web site is locked up."

"Oh. Damn. I assume we're executing recovery procedures?"

"Such as they are."

This confused Barton. He'd heard, time and time again, about the call lists and emergency procedures that assured business continuity in a crisis. "What do you mean, 'Such as they are'?"

"Sorry. That's my cynicism coming through. The fact is, those procedures are pretty badly out of date. I don't think we realized quite how out of date until thirty minutes ago."

This made Barton angry. "Wish you'd flashed that cynicism a little sooner. I've been taking everyone's word on this. I thought we were prepared for an outage."

Ruben, hearing the tone of Barton's voice, pulled back. "We're not completely unprepared, just not as prepared as we'd like to be. We've got great people on it. But the truth is that outages don't usually happen in a predictable way. Inevitably, we have to wing it a bit."

"And why are *you* calling to tell me?" Ruben's area had no operational responsibilities, thus would be involved in an outage only peripherally. Barton imagined his team voting on who the bearer of bad news would be.

"Because everybody else is kind of busy, frankly," Ruben answered. "Fenton and Cho are right in the middle of this. Ripley is at the data center, rebooting things. Juvvani and his team are trying to figure out what's wrong with the Customer Service systems."

"Cho? Do we think this might be some kind of security event?"

"I was coming to that." Ruben paused, as if to steel himself, before continuing. It was very unlike Bernie, that pause, and it communicated the gravity of the circumstances more than the words that followed it. A bolt of panic stirred the eggs Benedict digesting in Barton's stomach.

"We're receiving a continuous flow of e-mails at our Customer Service address," continued Ruben, "about three per second, each with no text in the body of the message and a one word subject line that says 'Gotcha.'"

"Gotcha?"

"Yes. It's like 'Gotcha, gotcha, gotcha, gotcha.'"

"What the hell does that mean?" Barton channeled his frustration into an exasperated hand movement, which promptly toppled his coffee cup. Hot liquid flowed from the table onto his lap.

"We don't know," said Ruben. "It could be a coincidence that Customer Service systems are down at the same time that we are receiving these e-mails, but . . . "

"But it doesn't sound coincidental, does it?" Barton stood, motioning to a waiter to indicate the spill and request his check.

"No," conceded Ruben. "This is the concern."

"Bernie, I need more information," Barton said. "I don't want to take people off their urgent duties, but at some point in the next hour or so I need a full update. Williams will get wind of this soon . . . "

"He has already . . . "

" . . . and I need to know what to tell him."

"I'll pull a group together, and we'll call you. How about 10:30?" Barton looked at his watch. It was 9:37 a.m. "Make it 10:15. There's no telling when Williams will call me. I'll hold off calling him until I hear more."

"I'm on it," said Ruben.

Barton hung up the phone. The waiter, rushing over to control the spill, also perceived the urgency of the call. He hurried the check to Barton, who quickly signed it and dashed out of the restaurant.

As Barton awaited the elevator that would take him to his floor, another call came in, this one from Graham Wells, IVK's VP of Legal Affairs and General Counsel.

"This is Jim Barton."

"Jim, we've got to reduce our legal exposure here." Wells's voice was an octave higher than usual.

"What do you mean, Graham?"

"We have to take dramatic action, signal that we've done everything we can."

"We *are* doing everything we can, Graham." The elevator arrived and Barton got on it. He pushed the button for floor 23. Two children got on too, with a woman apparently their mother. To Barton's horror, the two small boys pushed seven or eight buttons between the ground floor and floor 23 before the woman intervened. Barton immediately stepped out of the elevator, waited for the door to close, then pushed the up arrow again. All this time, Graham was speaking, not entirely coherently. Barton tuned into him again:

"Can we shut off power to the computer systems? Or cut the wires that go to the Internet?"

"We could, Graham, but I doubt that would be smart."

"Smart doesn't matter. What matters is what we can say in a deposition."

The elevator arrived, but Barton moved away from it to sit in a nearby chair.

"A deposition? What the hell are you talking about, Graham?"

"If this is a security incident," he continued, "we may be looking at legal implications. Customer lawsuits, shareholder lawsuits, government penalties, you name it."

"Because our Web site is down?" Barton said. But even as he said this, he knew it was more than that. His remaining optimism drained away, consumed in the heat of Wells's fear.

"If this is hackers—if hackers are stealing customer data—this is going to be *bad*."

"We don't know that yet, Graham."

"That's why we need to take drastic action. Listen, I just got off the phone with Carl. The last words he said to me were, 'Call Barton, make sure he understands the legal ramifications.' That's what I'm trying to do. And my official legal opinion is that we should shut down every computer in the place until we know what's happening. Can we turn off power to the entire company? I will now call Carl back and let him know that you and I have spoken."

Barton was shaken. "Thanks, Graham," was all he could manage. An elevator arrived and Barton dashed across the lobby to catch it.

Moments later he was back in his hotel room. His leg hurt where the coffee had burned it. It was a little after 10 a.m., not quite fifteen minutes until he'd get an update on the situation back at IVK. And he had no idea what to do. There were a dozen people he badly wanted to call, but all of them would be busy, and a call would only distract them. For a moment, he considered a call to Maggie then decided he didn't have time before 10:15. He shed the ruined pants and ran cold water over the coffee stain. For the analyst meeting, he'd have to wear pants from the day before.

At precisely 10:06 a.m., his cell phone rang again. It was, Barton could see from the display, Carl Williams. Barton took a deep breath and answered it.

"Jim Barton."

"Damn it, Jim, what's going on?"

"We're trying to figure that out, Carl," Barton said. He was trying hard to meet Williams's anxiety with calm confidence. "I've got a call with my team in . . ." he glanced at his watch ". . . eight minutes to get the latest."

"I just heard back from Wells. He said you were nonresponsive."

"Nonresponsive?"

"Look, never mind. Graham seems to have lost his mind. What do we know?"

"Well, call center systems are down."

"No kidding, those guys are just hanging out down there, chatting, drinking coffee. Costing us money."

"The Web site is frozen. And we're receiving suspicious e-mails. There are many possible explanations for the first two problems, some of them not very sinister, but the e-mails add a troubling aspect to the problem."

"Makes it seem like someone might be doing this to us?"

"Exactly."

"How can they? Don't we have a firewall?"

"Of course. We have many, but there's no such thing as perfect security."

"I don't want to hear—" Williams controlled himself. "I want an update as soon as you get a better idea, sometime in the next thirty minutes."

"Okay, right after my call in . . ." looking at his watch again, ". . . six minutes." Barton heard commotion in the background. Somebody was talking to Williams.

"Fine," said Williams. "I've got to go. Graham's calling again."

Barton closed his phone. He felt good about how that had gone. Unexpectedly, the interaction with the CEO had restored his confidence. The CEO had, in a backhanded way, expressed confidence in him. Now he just needed some good news from his team.

At exactly 10:13 a.m., Barton's phone rang again. He assumed it was the call he'd been expecting from his people, but when he looked at the phone display he saw that it was Williams again.

"Oh, boy." Barton had no idea why Williams would call back so soon, especially knowing that Barton was likely in a meeting, but he had a feeling that it would not be good news or helpful advice.

"Jim Barton."

"Hi, Jim, it's Carl. I've got Graham on the line. We've got another problem."

"What is it? I've got an update coming in two minutes . . ."

"I know, that's why we're calling now. We're not sure you should participate in the update."

"Huh? Why not?" Had they decided to replace him in the middle of a crisis?

"Jim, you've got a meeting with analysts this afternoon."

"Yes, I know, but that's not until after lunch."

Wells spoke then, explaining. "Jim, we've got disclosure issues if you talk to analysts in the aftermath of an event like this. Right now, you don't know what's happened. You don't know for sure, for example, that this event is security-related. Or that's what you told Carl, anyway."

"That's right," said Barton, not appreciating the implication that what he'd told Williams might be anything less than truthful.

"So," continued Wells, "we need to think about what we want you to know going into the analyst meeting. It might be best, if it's a security issue, that you don't know that yet when you talk to analysts."

"Carl, what kind of crazy, convoluted logic is this?"

"It's a legitimate concern," said Williams. "This may turn out to be nothing serious, or it might be very serious. We need to think about the representations you'll be able to make this afternoon without getting yourself and the rest of us in trouble. You're going to be on the hot seat. It might be best to have you go into it innocent of what's happening right now, or at least as innocent as we can make you."

"So you want me to just relax, enjoy the city, maybe take in a show?"

"Is there anyone you can delegate crisis response to?"

Another call was coming in on Barton's phone. It was 10:15 a.m. There was no time to think through what Williams and Wells were saying, but it felt wrong. Every fiber of Barton's being pushed back against what they were suggesting.

"The call from my team is coming in right now," said Barton.

"Don't answer it," said Wells.

"Don't answer a call from my team in a crisis?" Barton was aghast.

"Don't answer it," repeated Wells.

"Carl, this is wrong," Barton exclaimed. "This is my area of the company, my problem, and I need to be responsible for it. We can figure out how to manage the analyst meeting later. I can do that. I can handle it. Right now, my job is to fix this. Let me do my job."

"Graham?" said Williams.

"I advise against it."

Williams was silent. The digital alarm clock near the hotel bed clicked over to 10:16. Barton's phone beeped persistently as his team continued to try to reach him.

"Fine," Williams said finally. "Answer your call."

"Thanks, Carl," said Barton. He was about to switch over, but Williams wasn't finished.

"Make no mistake," said Williams, suddenly much angrier, "your butt is on the line here, Barton. I'm not a bit happy about this happening, not now, not at this time." He was venting. "Your timing could not be worse."

"Understood," Barton answered. For the second time that morning, he was shaken. Williams had said, "*Your* timing could not be worse." As if Barton had caused the outage. He gathered his wits and switched to the other call.

"Jim Barton."

"Hi Jim, it's Bernie. We've got you on speaker. Also present are Paul and Tyra. John Cho is down at his workstation, but he's with us on the line, as is Ellen Ripley, who's over at the data center, joining us by cell phone. Raj is with his guys working on Customer Service systems, so he's not with us; we can call him on his cell if we need to, though."

"Great, what do we know?"

Paul Fenton spoke up. "There are several things going on. You know about the e-mails, I think."

"Yes."

"The Web site is locked up because of what appears to be a rather sophisticated denial of service attack. We have software to defeat ordinary DoS attacks, but this one is coming from many locations and is attacking with a pattern of traffic designed to defeat our countermeasures. We are working on that and think we will be able to neutralize the threat in the next few minutes. The Web site should be operational after that.

"The thing that has us most puzzled is the Customer Service systems shutdown. We don't know what's causing it. Ellen tried rebooting everything that has anything to do with those systems, but it hasn't helped. Transactions against the database are returning an error code. We can't add new or retrieve existing customer records. That could mean there's something wrong with a transaction that's got everything jammed up behind it. Or it could mean the database is corrupted."

Barton interrupted: "Do either of those possibilities indicate that an intrusion has occurred?"

"Not necessarily. If it's a problem transaction, that is most likely an internal software problem. If it's database corruption, someone could have caused it, but it could also have happened without any malicious involvement."

"John, what do you think?" Barton braced himself for the possibility of anger in Cho's response.

Reuben spoke for Cho: "John thinks it's malicious, but that's his predisposition. He thinks someone has exploited the security hole he's been worried about." Cho, though supposedly on the line, did not elaborate.

"The security hole," said Barton, "that we've proposed addressing with a fast-track upgrade project." The project Barton had shot down while he was head of Loan Operations.

"That's correct."

"So what do we do?"

Fenton appealed to Ripley, his network operations team leader: "Ellen?"

"We can probably deal with the database corruption issue by going to a backup. But it might happen again. And we'll lose some data from yesterday afternoon if we revert to a backup. We'll have to re-enter all that data. Also, going to a backup may not solve our problems if they are due to an intruder. If it's a hacker and he's left malicious routines on our computers, they are likely also present among backup files.[1] The problem might just recur."

"Can't we tell if there are files on our computers that shouldn't be there?"

"We should be able to," a new, deeply annoyed voice broke in, "but we can't." Barton recognized it: John Cho.

"Explain."

There was a silence, then Cho started again. "We're supposed to keep careful records of all files introduced into production. But we haven't."

"Why not?" Barton asked.

"Because sometimes idiots in the applications groups rush changes in without going through the proper procedures—"

"There are good business reasons to do that sometimes," interrupted Tyra Gordon. "And it's not like others are not on board when we do it. Everybody knows what we are doing when we do that."

"I *never* agree to it," said Cho.

"It must be nice," Gordon said, "never to have to operate under pressure from a customer . . ."

"That's a load of crap," said Cho, "I advise you to come down here and try this kind of pressure . . ."

"Hey!" Fenton shouted. "People. Let's stay on point here."

"So," concluded Barton, "somebody in Tyra's group put in a change without following procedures?"

"Raj's group, actually," said Gordon, "it's his systems having the problems."

"But the rush-a-change-into-production thing is not unique to Raj's group," said Fenton. "It's been a sore point for years. We have careful procedures, but when a big customer screams for a change, procedures sometimes get circumvented. Outside IT, change control procedures tend to be viewed as a form of bureaucracy. Business unit managers sometimes force through quick changes that circumvent change control."

"Like, for instance," interjected Cho, "the VP of Loan Operations." Barton had a vague memory of browbeating Davies into such a quick change in the not-too-distant past. *I deserved that*, thought Barton, deciding to let Cho's not-so-subtle barb pass.

"I get it," Barton said.

Fenton continued: "As Tyra rightly says, we all know it goes on, and we all acquiesce. In the minds of many on the business side, this is justified if it makes a customer happy. It's a business trade-off, in effect."

"The bottom line is that we don't know if bad guys are involved," Barton concluded.

"That's right," said Fenton.

Barton heard a commotion in the background, some quiet talking. Fenton came back on the line: "The DoS attack is under control and the Web site is back up."

"Well, I suppose we can call that some kind of progress. Is there any other way we can tell if bad guys are involved?"

"Maybe," said Fenton. "It depends on how careful they were, if they were there at all. John's working on it."

"No smoking gun yet," said Cho, now speaking in more measured tones. "If it's bad guys, they're very, very good."

There was more commotion in the background. Barton heard a cell phone ring. Fenton answered it. Barton couldn't quite make out what was being said, but Fenton came back after less than a minute.

"Raj's people have figured out what the problem is. We'll have Customer Service back up and running in about ten minutes."

Barton felt relief that he knew was not yet justified. "Great. What was the problem?"

"Apparently a database index file had been somehow renamed, and another substituted in its place. All they have to do is rename the files back to how they were before, and we should be fine."

"Files renamed. Can that just happen?"

"I don't know," said Fenton.

"Not likely," said Cho.

"Let's be careful here," said Gordon. "There's danger in overreacting as well as underreacting."

"Okay," said Barton. "I've got to update Williams. I want us to meet again in sixty minutes, say, at 11:15 a.m. I need two groups, working on two different tasks. Paul, you, John, Raj, Ellen—I need your best sense of whether there's been an intrusion, and what we need to do about it, whether we're sure or not sure. Bernie, you and Tyra and whoever else you think might help who isn't working on what's happened here, I want you to develop some advice for me on how to handle the analyst meeting, which is at 2 p.m. Okay?"

"Can you cancel the analyst meeting?" asked Ruben. "Say you've come down with food poisoning?"

"Might seem suspicious, especially if word of what's going on here has leaked out. What if someone preparing for the meeting this afternoon has been having trouble accessing our Web site this morning? Or what if some call center employee has called a friend or sent an e-mail about what's going on? Word might be out already. But everything's on the table. If you think canceling the meeting is a good option, explain why. Okay?"

"Will do," said Ruben "Anything else?" All lines were silent; no one said anything. "Signing off, then." Barton snapped his phone shut.

Barton immediately called Williams with an update. Williams listened, said little. Barton hung up and ordered coffee from room service. He pulled on yesterday's pants. Then he sat down to put together his

own ideas about what he might say at the analyst meeting under various scenarios. His leg hurt a lot, but his head hurt even more.

Thursday, June 28, 11:21 a.m. . . .

Paul Fenton had just finished his update. Juvvani, Gordon, Cho, and Ripley were also on the line. The meeting to recommend an approach to the analyst meeting had been moved back fifteen minutes, to give that group time to send Barton some PowerPoint slides. Gordon, part of that group, was sitting in on this meeting to make sure she had the latest information on what had happened, as an input into what to say at the analyst meeting.

The facts so far: There was still no smoking gun that indicated an intrusion, although Cho was convinced that was the explanation. If it had been intruders, they had been deep enough into the IVK production computers to rename database files, which meant they could have also stolen customer data or corrupted it subtly. Loan applications asked for credit card numbers to be used in credit checks, but, fortunately, IVK did not retain that information. Unfortunately, the company's databases did retain Social Security numbers and other information useful to identity thieves.

"I think we need to disclose that something has happened," said Cho. "I think we're legally obliged to, in fact."

"We should get legal advice on that," said Fenton. Barton thought of Wells's incoherent state when last they spoke. Fenton continued: "My interpretation of our obligation is that we have to disclose if we know we've lost customer data."

"Actually," said Cho, "it's if we *suspect* we have."

Juvvani weighed in. "So what does that mean? You suspect we have, John. Maybe I don't."

"So you think those files just renamed themselves?" Cho asked.

Gordon came to Juvvani's defense: "We don't know what people do on the night shift. We don't know a hundred other things. Just because we can't think of another innocent explanation doesn't mean there isn't one.

How often before have we seen something happen that we think can't happen, only to discover some complex, idiosyncratic explanation?"

"Yeah," said Cho, "but renaming database files—that's pretty specific. How would that happen innocently?"

"Like I said—" Gordon began, then stopped.

"Might it be an inside job?" asked Fenton. "Could someone with approved access have done it? Is this somebody's idea of a joke that got out of hand?"

"I don't know," said Cho. "And I've been going over the logs pretty carefully. I don't think we're going to know. I have to admit, it seems implausible to me that someone could have done this without leaving any sort of a trail. But renaming a database index file . . . that's just not the sort of thing that happens by accident."

"So," said Barton, "what you're telling me is that we are not going to know whether this is a security event by this afternoon. That we may never know."

"Never is a long time . . ." said Fenton.

"That's what *I'm* saying," said Cho. "Unless we stumble onto something that tells us. I'm going to keep looking, but I've looked in most of the obvious places already."

"What do we recommend doing in the aftermath of this event?" asked Barton. "Williams is going to want to know what we're planning to do to avoid a repeat of this."

"Well," said Cho, "obviously we accelerate the security project we've got in motion. Maybe add some more to it—I've got a wish list of stuff. Maybe Williams will sign off on what we really need now. And, of course, we've got to begin following our procedures better. Maybe in the aftermath of this problem, people will understand better why we force procedures on them. Ellen's got a recommendation too, that I totally agree with."

"Ellen?" said Barton.

Ripley sighed, then launched into an explanation. "There's an additional concern. We can take the actions John is proposing, and that will close a lot of the possible holes in our security that we know about. But if—and as we've been saying, it's a big *if*—bad guys have been inside our production systems, what we've experienced so far might not be

the full extent of nastiness they have planned for us. We can't tell what should be on our systems and what shouldn't be. So there might still be some bad code on our machines. Closing the holes in our security doesn't help with anything bad that's already on the inside."

"Okay," said Barton. This sounded like bad news, but so far he'd heard no recommendation. "And so that means we should . . . ?"

Ripley sighed again. "I think we need to shut down our production systems for a period of time, say three or four days, wipe production servers clean, and rebuild the production configuration from development files. It's unlikely, though not impossible, that the bad guys, if there are any bad guys, reached into our developers' machines. We should be able to put our production systems back together with only what *should* be there, and then we can keep tight control on them thereafter by following our change control procedures better."

"By shutting down our production systems," Barton asked, "you really mean shutting down the company's operations for that long?"

"Yes," conceded Ripley. "Mostly. We could take calls and do some things manually. But there's no doubt it would be a big deal."

Cho spoke: "We dust off and nuke the entire site from orbit. Eradicate any nasties left on our production servers. But it's really the only way to be sure."

"Can we," asked Barton, "set up parallel systems built from development files, *then* switch over to those before we take down our production systems? Wouldn't that help us avoid a shutdown?"

"Yes," answered Ripley, "we could do that. It would be expensive, because we'd have to buy or otherwise acquire additional space and equipment. And it would take time. Which is the biggest problem with that idea. If the bad guys have more difficulties planned for us, that's time—definitely days, maybe a week or more—in which their plans can execute. Waiting might mean we have more problems."

"Just so I've got this clear," said Barton, "You want me to go to Williams and tell him we need to shut down production computers as soon as possible, and keep them down for, what, three to four days?"

"That's about what it would take," said Fenton. Barton realized that his team had discussed it already and agreed on this plan of action.

"You realize that this is not our decision," said Barton. "It's Carl's decision. And I've got to tell you, I don't think he's going to like it. Nobody outside IT is going to like it."

No one said anything.

"Any ideas," Barton asked, "about how we frame this shutdown from a PR standpoint? What we say to our customers and the public about why we're shutting down for four days?"

Still no one said anything. It was Barton's turn to sigh. "Okay," he said. "Let me think about it."

He flipped his phone closed and opened an e-mail from Ruben that contained a PowerPoint slide attachment, a plan for how to handle the analyst meeting.

He looked at his watch. It was already 11:44 a.m. The meeting was in a little more than two hours, and he still had to get downtown.

REFLECTION

How should Barton handle the meeting with the analysts? What questions should he be prepared to answer and how should he answer them?

How vulnerable is your company (or a company that you know) to a denial of service (DoS) attack or intrusion? What should be done about such vulnerabilities?

Why can't perfect IT system security be achieved? If security can never be perfect, how should you manage against malicious threats?

NOTES

CHAPTER TEN

1. For a fictionalized account of the weapons hackers use to break in, see Carolyn Meinel, "How Hackers Break In . . . and How They Are Caught," *Scientific American*, October 1998, 98–105.

GLOSSARY OF ACRONYMS AND TERMS

Apache	A public-domain, open source Web server
A/P	Applications portfolio
APM	Agile project management; also applications portfolio management
APP	Aggregate project planning
BGP	Border gateway control
CEO	Chief executive officer
CFO	Chief financial officer
CIO	Chief information officer
CMM	Capability maturity model
CORBA	Common Object Request Broker Architecture
CPM	Critical path method
CRM	Customer relationship management
COO	Chief operating officer
CQ	Competes [versus] Qualifiers
DBA	Database administration
DBMS	Database management system
DoS	Denial of service
DP Era	Data processing era
EAI	Enterprise application integration
ERP	Enterprise resource planning
IDS	Intrusion detection system
IPO	Initial public offering

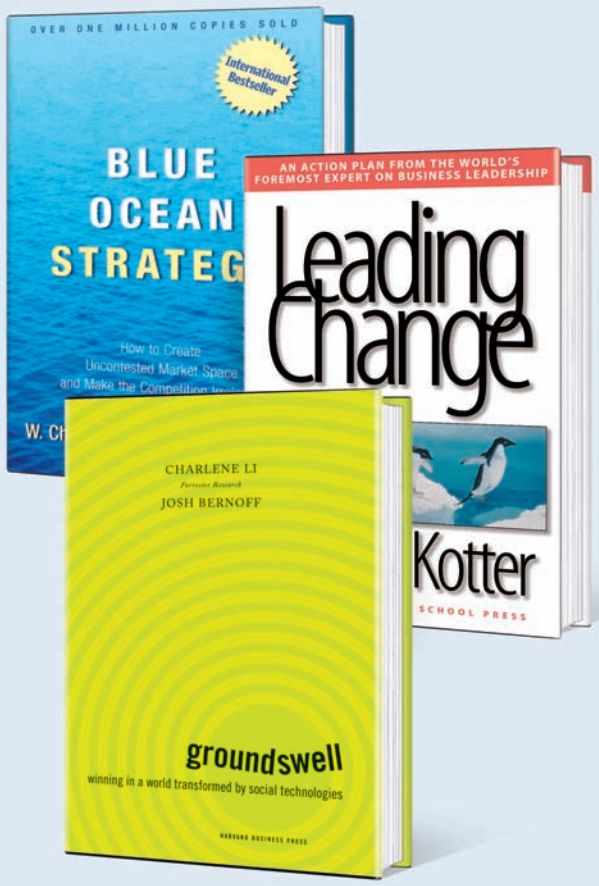
IR or IRP	Infrastructure replacement project (as used in this book)
IT	Information technology
ITIL	Information technology infrastructure library
Java	A high-level programming language developed by Sun Microsystems
KWYDK	"Know what you don't know" (as used in this book)
Linux	An open source operating system
OCI	Option creating investment (as used in this book)
Oracle	Large software company, focused on database products
OSI	Open systems interconnection
PC	Personal computer
PDA	Personal digital assistant
PERL	Practical Extraction and Report Language
PERT	Project Evaluation and Review Technique
PGP	Pretty Good Privacy
PLM	Product lifecycle management
RFP	Request for proposal
ROI	Return on investment
SaaS	Software as a service
Sabre	Semi-automated business research environment
SLA	Service level agreement
SOA	Service-oriented architecture
SQL	Structured query language (originally SEQUEL: structured English query language)
SSL	Secure sockets layer

SYH2DP	"Sometimes you have to duck a punch" (as used in this book)
TCP/IP	Transmission Control Protocol/Internet Protocol
TPM	Traditional project management
Unix	A multi-user, multitasking operating system
UWGDF	"Understand what got Davies fired" (as used in this book)
VPN	Virtual private network
YWLOY	"You won't last one year" (as used in this book)

THE ANSWERS YOU NEED,

WHEN YOU NEED THEM

DOWNLOAD **BOOK CHAPTERS** NOW



NOT ALL BUSINESS CHALLENGES ARE CREATED EQUAL.

Some require detailed analysis and others demand a thoughtful solution—but in a quick and easily accessible format.

Now you can get instant access to the answers you need by downloading **individual chapters** from our most popular books, including:

- *Blue Ocean Strategy* by W. Chan Kim and Renée Mauborgne
- *Leading Change* by John P. Kotter
- *Groundswell* by Charlene Li and Josh Bernoff
- And many others

The solutions to your toughest challenges are just a click away.

HARVARD BUSINESS Press

LEARN MORE ABOUT HARVARD BUSINESS PRESS CHAPTERS:
www.harvardbusiness.org/press