Additional Case 5

Queensland Rainforest Resort

Janine S. Hiller
Virginia Tech

Sam A. Hicks
Virginia Tech

France Belanger
Virginia Tech

Nancy G. McGehee
Virginia Tech

Built in 1987, Queensland Rainforest Resort (QRR) was the first Australian resort to be developed by Adventures Hotels and Resorts Inc., whose headquarters office, along with two additional resorts, was located in California. Adventures Hotels and Resorts (AHR) was a hospitality company committed to showcasing and preserving the extraordinary destinations in which their properties were located. On the homepage of the resort was a statement by QRR's executive director, Abe Grant, which read as follows:

> Explore wild Australia in luxurious comfort in our award-winning resorts. We are committed to sharing Australia's beauty with the world while protecting it. Our properties are managed within strict environmental guidelines; we are committed to sustainable tourism management practices, to energy-efficiency, recycling and waste management programs. From the red heart to the rainforest, from canyons to the Reef, here are landscapes to ravish the senses and refresh the spirit.

QRR was located two hours north of Cairns, Australia, in the Daintree Rainforest, and was the only place in the world where two World Heritage listed environments existed alongside each other, or as the locals said, where "the rainforest meets the reef." QRR was a full-service luxury resort that offered both a lodge with deluxe accommodation rooms and private cabins set farther back in the rainforest. All rooms and cabins had direct access to the white sand beach.

Every element of QRR was designed to take advantage of the natural setting while staying attuned to ecological and sustainable growth ideals. For example, the minimal amount of timber removed for the development of the resort was used to build the cabins and lodge; a local spring provided all the water for the resort; plumbing and water filtration systems had been developed using state-of-the-art conservation techniques; all the soaps and detergents used at the resort (both in rooms and in the restaurants) were biodegradable; and all indigenous flora and fauna located in or around the 450 million-year-old rainforest surrounding the resort were treated as "honored guests," including tropical birds, tree kangaroos, and monitor lizards.

Amid the natural beauty, however, not all was well. Although the resort attracted visitors from all over the world, in part due to the strength of its presence on the Internet, the global downswing in international travel, fueled by the decrease in visitors from the United States, was a significant problem for QRR. Everyone was tense about the decrease in visitors, and things were very tight. Adventure Hotels and Resorts (AHR), the corporate headquarters located in California, had made it quite clear that unless profitability increased, some real cost-saving measures would have to be instituted. Lost jobs and cutbacks in service were all possibilities in the near future if things did not show improvement. Part of the corporate strategy to save money and increase profitability was to use technology to improve and streamline both internal and external functions. Although the resort's

 This case was made possible in part by a grant from the Boeing Chartable Trust Foundation to the Center for Global Electronic Commerce, Pamplin College of Business, at Virginia Tech.

appeal was based on the natural environment, QRR sought to be thoroughly modern and efficient, especially in the area of information technology.

QRR's information technology evolved, as with many resorts, from a few bulky computers at the accountant's desk to tabulate accounting data and print bills to a highly sophisticated technology environment companywide. In addition to standard accounting and payroll systems, QRR had adopted point-of-sale systems for its restaurants, automated credit card processing systems at all areas receiving guest payments, e-mail systems within the resort and across the corporate environment, connections to the Internet, and even Web registration and payment services.

At QRR the information system function reported to the vice president of operations. The day-to-day IT operations were managed by Peter Myers, the information technology director. However, because of limited resources, QRR made a strategic decision four years ago to outsource a large part of the information systems function. This was triggered by the need for an online reservation system. Peter evaluated and discussed the possibility of in-house development with the executive committee; but in the end it was felt they had neither the resources nor the expertise to make it happen. Instead QRR contracted with CibCo, an outside company, to provide online reservation functions.

Jessica Austin was the CibCo account representative for QRR. In her sales presentation to QRR executives, Jessica suggested that many more existing functions could be outsourced at lower costs than in-house development and greater efficiency. QRR agreed. Today, CibCo had a contract to host and maintain the Web site and hosting applications at QRR, including inventory control, payment, and payroll applications. However, a few IT services were managed centrally at AHR, such as the e-mail server functions.

At QRR, the basic systems environment was a series of three Ethernet LANs connected through a router and a bridge. There were three local servers. One was used as a database server accessed by all stations and point-of-sale locations at the resort while another was used as an application server, running applications such as front desk registrations, phone reservations, and the local accounting applications. Finally, the resort had its own Private Branch Exchange (PBX) for handling all of the phone connections for the resort.

THE LETTER

Caitlin Murphy, vice president of customer relations at Queensland Rainforest Resort (QRR) had just read a letter she received from a particularly loyal, but also particularly irate, customer regarding a recent visit to QRR. "Maybe I should not have transferred from the corporate office of AHR," she thought to herself. "Australia seemed such a beautiful place to live for a few years and a good place to distinguish myself for further advancement."

She decided to read the letter again:

Dear Queensland Rainforest Resort Management:

My family recently spent our third vacation at your property, traveling all the way from the United States (California), and I have to tell you that it may be our last. While we always enjoy traveling to the Daintree Rainforest, this last trip was dampened by a number of problems related to our interactions with the Queensland Rainforest Resort. Our problems with the resort all began when we arrived at the resort and found that there was no reservation in our name, even though we registered online a full 6 months ahead of time and had a copy of our confirmation e-mail. Your front desk staff was very nice, and luckily there were rooms available, but there were some pretty tense moments until we found that out for sure. Things then proceeded to go well for a day or so, but we ran into additional trouble when we decided to eat at the Billabong. Each time we visited the restaurant our order was either wrong, or cold, or slow to arrive. The waitress was very apologetic, even "comped" our meal the third time, but she seemed to be frustrated by the system she was using to place our orders.

The rest of the visit went well, but after we returned home, our problems seemed to follow us. Almost as soon as we got home we began to be inundated with brochures, e-mail, and telephone calls from similar types of other high-end resorts; it appeared that Queensland Rainforest Resort had sold our personal information, which we found very disappointing. Next, several of the incidental charges we incurred at the resort (meals, room service, long distance, spa visits, the reef tour) were not charged to our credit card until almost 6 months after we returned from our trip. When we called our credit card agency, they informed us that it had taken that long for Queensland Rainforest Resort to submit the charges. When we e-mailed the accounting department about the problem (numerous times) we never received an answer. Instead we received numerous undeliverable e-mail responses.

All these things were an inconvenience and a bother, but nothing prepared us for the final straw: 8 months after the trip, we were victims of identity theft! Someone spent over $25,000.00 on our credit cards. Luckily they were caught and prosecuted, but the authorities traced the source of the problem to your resort. In addition, a family we met from England with whom we have maintained e-mail correspondence had similar problems to ours, and they have suggested that we all should receive some form of compensation. I have to say I agree with that idea, and have been contemplating calling my lawyer, just to see what our rights are. I find it very distressing that a resort that bills itself as a luxury experience, and charges room rates accordingly, has such problems with its information technology.

Let me just say that we are incredibly disappointed, because we have LOVED our trips to your resort over the years, but we cannot justify returning if our interactions continue to result in so many problems for us. I hope that my complaints will result in some improvements. If you are unable to demonstrate changes to us soon, we will have to begin to search for a new vacation destination for next year, as well as recommending to our friends and colleagues that they refrain from visiting your resort.

Sincerely,

Spencer Benjamin, M.D.
Los Angeles, CA

Obviously, there were numerous issues that needed to be addressed. While Dr. Benjamin was the only customer to complain about all of these issues, many customers had complained at different times about various problems related to the resort's online registration and reservation system, restaurant orders, credit card transactions, and e-mail. As a new employee, Caitlin Murphy herself had been the victim of a slow payroll system when she had to wait almost two months before receiving her first paycheck. While the problems seemed a bit overwhelming, Caitlin knew something had to be done.

DATA COLLECTION

While Caitlin Murphy was beginning her investigation into Dr. Benjamin's complaint, information technology was at the center of attention in another part of the resort as well. Martha Hines, marketing director for QRR, was in her office after just returning from a seminar in Orlando, Florida, entitled "Make the Most of Your Customers: One-to-One Marketing and Other Profit Enhancing Techniques." She was excited to bring back ideas to incorporate into the new marketing plan. In fact, Martha had been energized by the conference ideas. At the last QRR executive committee meeting, it had been decided to task the marketing department with creating an aggressive plan to increase guest nights in response to the sagging bottom line. According to what the conference speaker said, it would seem that QRR was sitting on a gold mine of information. And, by using the Internet, she could reach millions of people for an extraordinarily small investment. If she could put some of these ideas to work, then QRR could increase its profits even without renting any additional rooms! Martha could taste the promotion that she would receive if she could pull this off.

The list of new marketing techniques included the following possibilities:

- Use e-mail lists from private vendors to send information about QRR all over the world.
- Trade e-mail lists and guest information with others who also market to resort and ecotourists.
- Sell e-mail addresses and other guest information, such as the address of customers, to other related businesses such as outdoor equipment manufacturers and wildlife groups.
- Subscribe to an advertising program to place pop-up ads for the resort on surfers' computer screens.
- Collect information about the Web sites that guests access while staying at the resort. Use this information to create a database of products and services that would be targeted to the guests.

All that was needed now was to pull together a presentation to the executive committee. Martha called together the marketing staff for a work session. To her surprise, not everyone was as excited and enthusiastic as she was about the ideas, and in fact Terry Travis, one of her marketing specialists, was an absolute spoiler. "I don't see how you can even think about this! What you are doing is sending spam. I don't want to become a spammer; I absolutely hate the spam that I receive now. I'd rather quit than work on this. And I don't see how you can violate the confidence of the customers. If it were me, I wouldn't come here if I knew that you would use my information like that."

Samantha Hu also spoke up: "This company stands for high ideals: preserving the environment while still opening it up for visitors. I think these new marketing ideas violate the overall values of our company. Besides, what if it backfires on us? Did anyone else besides me receive that memo about the disgruntled customer from the States? I think his name was Benjamin—who was outraged because his information was somehow leaked from QRR—including his e-mail address? At some point, customers will revolt and take their business elsewhere, and that's really not what we need to see happen right now."

But Lee Woods disagreed, saying, "High ideals are all well and good, but not if you are out of a job. And, while you are on your high horse, someone else is already out there taking advantage of the data and customer information. Face it; we don't have any privacy anymore, and we would not be doing anything that other resorts aren't already doing. Everyone expects you to use the information already."

BACKDOOR POLITICS

Unaware of the brewing controversies in other resort departments, Jody Antopolis had information technology concerns of her own. "Peter, you may want to sit down to hear what I am about to tell you. We have a huge problem, one that could cost a lot of money to fix." Jody Antopolis walked into the office of her boss and IT director, Peter Myers, and proceeded to tell him about her discovery of a hole in QRR's reservation system and Web site.

At first, Jody was sure that it must be a mistake. The company had paid an arm and a leg for the e-commerce Web site and reservation system from CibCo. Jody ran the program again, just to make sure that it was not an aberration. "No, there it was," she thought. "CibCo must have left a backdoor in the program so that they could disable it if payments were not made on time." She remembered the discussion about the backdoor and the jokes around the IT group about electronic warfare between the two companies if a disagreement broke out. Now, anyone with an advanced knowledge of the programming language could easily access QRR's customer information, including addresses, names of children, and e-mail addresses. "Thankfully," she thought, "the credit card numbers are encrypted, so at least they are protected." It was at this point that Jody decided to report the problem at once to Peter.

She took a deep breath and continued her story. "So, I am afraid that we need to shut the system down, Peter. I believe I can get my group to work around the clock to reinstall our old in-house system. It won't allow for reservation updates, and it won't link the information to the database created by the new system, but it is secure, I am sure of that."

"Now hold on, Jody," said Peter. "I am not at all convinced that we should shut the system down. After all, it would take a person with a considerable amount of knowledge to break in. And it hasn't happened yet, has it? I think that we should continue to use the system until such time as we actually know that someone has broken into it. Really, all we have now is a possibility of the information being lost, and if anything happens, it will be CibCo's fault, not ours."

Flabbergasted at Peter's curt response and quick decision, Jody left the office. She now had a decision of her own to make. By simply doing what she was told, she knew she was participating in a breach of trust with QRR's customers. On the other hand, if she were a QRR guest, she would not like to find out that her private information had been compromised in that way. Should she stay the course and follow her boss's instructions?

Jody was suddenly reminded that just yesterday she had been copied on an e-mail memo informing the staff about a particularly troublesome complaint letter. The guest, a doctor from the United States, had experienced an awful series of IT-related problems after a recent stay at QRR. She had only skimmed the letter at the time, but she was sure she remembered that the guest had experienced an influx of spam shortly after his visit. Could someone from CibCo be accessing the QRR Web site and selling the data? Just the thought made Jody sick with worry. This pointed to a second option for her decision about the hole in the system. Jody could send e-mails to all the guests in the database. "After all," she thought, "they have a right to know, and perhaps this would bring pressure on QRR to fix the problem."

EYES ON THE INSIDE

The meeting with Jody was disturbing, but Peter had other issues to attend to, and he needed to particularly focus on the report that he was scheduled to give at the next executive committee meeting. As he turned back to his work, his mind wandered back to the meeting that had started it all.

Exhibit 1 QRR Computer Acceptable Use Policy

All employees at QRR granted access to information systems and networks owned or operated by QRR must follow company policies, and local, district, and national laws. Access also imposes certain responsibilities and obligations. Acceptable use always is ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

The company considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information resident on its systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations.

General Guidelines:

In making acceptable use of resources you must:

- use resources only for authorized purposes.
- protect your account and computer from unauthorized use. You are responsible for all activities on your account or that originate from your system.
- access only information that is your own, that is publicly available, or to which you have been given authorized access.
- use only legal versions of copyrighted software in compliance with vendor license requirements.
- be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

In making acceptable use of resources you must NOT:

- use another person's computer, account, password, files, or data without permission.
- use software to decode passwords or access control information.
- attempt to circumvent or subvert system or network security measures.
- engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to university data.
- use corporate systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
- make or use illegal copies of copyrighted materials or software, store such copies on university systems, or transmit them over university networks.
- use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or account.
- waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- use the company's systems or networks for personal gain; for example, by selling access to your account or to systems or networks, or by performing work for profit with company resources in a manner not authorized by the company.
- engage in any other activity that does not comply with the General Guidelines presented above.

The purpose of the meeting was to review CibCo's contract concerning the outsourcing of certain IT functions and to discuss projects for the upcoming year. During the discussion, Abe Grant, executive director of QRR, had asked Jessica Austin, CibCo's account representative for QRR, a provocative question: "Is it possible to monitor all of QRR's employees? How about employees' general use of e-mail and the Internet?"

"Of course," Jessica replied. She went on to describe various options for monitoring employees' use of the Internet. Although Peter recommended moving more slowly, Abe agreed to the service and asked for it to be implemented immediately. Peter was assigned the responsibility of summarizing the monitoring reports for Abe, and making a presentation to the executive committee about the status of the new monitoring (see Exhibit 1).

Now, a month later, Peter was reminded of that meeting as he reviewed the first set of reports. Jessica's team had provided him with a log of who sent e-mails to whom and when, with the subject line's content. The content of the e-mails was not included in the report. Peter glanced through the

report and saw that a certain Mike Howell in front desk operations sent many "lunch together?" e-mails to a Julia Robertson in food and beverage. "An office romance, no doubt," Peter reflected. Should he report this? What if one of them was married? What other information is in these e-mail logs? As he thought about this, Peter realized he might not be able to delegate the job of summarizing these reports to one of his employees, as he was first tempted to do. What if they used the information in the wrong way?

Still puzzling about what to do, Peter continued looking at the Web access reports. These reports were in a different format. Each user account was listed in alphabetical order, with the user's top five Web sites ranked according to the number of times accessed, and then the top five Web sites ranked by quantity of time spent on those sites. Immediately, Peter knew that this was going to be an ugly job. He browsed through the lists and found three accounts where the top Web site use seemed excessive. He then found to whom the accounts belonged and visited those sites. The following is a summary of his major findings and thoughts:

- Maria Jones, a reservationist, went to an online games site every day for almost one hour.
- Anthony Vega, a food and beverage manager, looked at a stock market Web site very frequently, although he spent much more time overall looking at a food and beverage equipment auction site.
- Jared Michaels, a maintenance manager, went mainly to an adult entertainment Web site where pictures of nude or almost-nude young women were plentiful, and were available for downloading. Peter made a note to see what other suspicious "files" might be saved to Jared's computer.