PRIVACY PLANNING AT HALOH FOUNDATION

Ingrid Splettstoesser-Hogeterp
York University
TORONTO, ONTARIO, CANADA

Abstract

Haloh Foundation, a fictitious charitable organization, has worldwide operations exceeding $800 million annually. After experiencing a phishing attack, the federal Privacy Commissioner orders Haloh to prepare and document an updated privacy policy and assess its privacy practices.

The multi-part case will be useful to instructors teaching privacy principles, business ethics, management controls, management information systems or assurance services, as it focuses on basic principles of privacy protection, and on controls over data. The case could be taught in segments or in its entirety. Qualified case user can request a detailed teaching note from the author.

KEY WORDS: Data privacy, privacy protection, information systems controls, password management

PART 1 - HALOH’S UNWELCOME BRUSH WITH PUBLICITY

Jhanna, the Vice President (VP) of Marketing was in a panic. How was it possible that a hacker had obtained the email addresses of their donors? She knew about phishing, having received enough of that kind of junk mail herself. However, she had never dreamed that someone would attack their precious donor information. What if the donors sued the charity?

The day had started normally enough. Jhanna had been thinking that she was glad that the annual fund-raising drive was over. This was the first year that donation receipts were prepared and emailed in Pdf-format within two business days of receiving the donations via Haloh’s secure web site. Preparing receipts was boring, but yet important. An inaccurate receipt could send a donor into a fury.

Ten full-time staff members in several departments spent every spare minute preparing and sending receipts. Jhanna had carefully screened and then hired four new part-time employees (all past volunteers) for mailing most of the receipts. In the past, receipts were printed once a month by Haloh’s information systems department and stuffed into envelopes by volunteers. Haloh had switched to the new system because email was considered a convenient and effective way of communicating and staying in touch with the donors and in promoting Haloh’s goals. The problem was that sending individual receipts by email on a continuous basis was much more costly than sending printed receipts once per month, even when including the cost of postage. Jhanna now regretted that she had allowed herself to be talked into the switch.

The internet donation information had also been passed to the accounting department, where someone had to record all donations again to enable reconciliation with cash received, update the donor pledge amounts, and prepare reports of donations for the annual charitable donation return. Weren’t computer systems supposed to save time and money, rather than requiring typing the same donor payment information more than once? Couldn’t programmers do something to pass this information across? Spending money on part-time employees to send donor receipts meant there was less money for her marketing team in the coming year. Jhanna had already been feeling grumpy when she listened to
the voice message on her telephone. The voice of George, the Supervisor of Client Relations provided disturbing news.

"I've had a telephone call from one of our long-time donors. It seems that he received an email that claimed to be from Haloh’s customer support, asking him to update his credit card information. Now, he says, he cannot log on to our web site. Could this be one of those phishing emails, you know, that grab personal information? He is wondering how these people got his email address. I'm going to call Quiang in computer support and see if he knows any more about this."

Not a good start for the first Monday morning of the New Year. Jhanna’s head hurt. If this hacker had managed to get access to the email addresses, what else might he have had access to? Was the company’s computer system not up to speed? Had he accessed any of the operational data? There was payroll, accounting ... She wasn’t sure how everything was organized. It was time to talk to Ruth, the Corporate Controller, before she started grilling Quiang, the Information Systems Manager. Jhanna drummed her fingers on the desk. She might as well face the problem now, she thought, as she got up to head down the hall.

Ruth was running her fingers through her curly grey hair, her visible worry habit. Jhanna could see her talking to Quiang, who was sitting across from her desk in her office. Ruth seemed to be talking in rapid bursts as Quiang repeatedly shook his head or shrugged his shoulders. Ruth looked up sharply as Jhanna entered her office and directed her quick words at her.

"Email files, who would have thought. They're on our intranet. Quiang says our router is in working order and the firewall is current, and there were no alarms in the last few days, but he'll call the firewall and router suppliers and see if there is anything else. Blast! As if we need extra work right now!"

Jhanna listened quietly as Ruth and Quiang continued to run through possibilities, all ending in a blank. Jhanna’s mentally ran through multiple alternatives, thinking what she and her staff could do to mitigate the damage. As marketing VP, it was her job to respond quickly to matters that affected Haloh’s donors.

"I think what we need to do is send out one of those warning emails right away. I’m going to draft one and you let me know if the wording is alright. You know, telling donors not to answer emails that ask about their personal information."

Jhanna raised her eyebrows and looked at Ruth, as if asking for acquiescence. Ruth nodded absent-mindedly and Jhanna went off to look for George, to see if he had any additional information about what had happened. George did not have the details, but after contacting the affected donors, he obtained the email address of the party that had sent the phishing email, as well as a full copy of the offending message. This gave Jhanna the details she needed to include in the warning email message, which Ruth agreed to and George sent out to all donors within the hour.

During a meeting two days later, Ruth informed the management team that Quiang had discovered the entire donor email mailing list (in plain text) posted on Haloh’s public website. Although the list could not be accessed via any menu links on the website, it could be read by anyone browsing the website files. All a hacker had to do was to list all folders of each section posted on the website. The “Contact Us” section included the file ‘decemberlist.doc’ that included email addresses and names of some 3,000 active Haloh donors. Ruth then questioned all employees how they used email mailing list files. No one at Haloh admitted to posting the text file and there did not seem to be a way of finding out who had done it. Whoever it was, had probably thought of it as a convenience for sending emails.

The local newspaper got hold of the story and splashed it all over the front page – “Haloh Foundation’s donors subjected to phishing scam – beware of where you donate your money!” The next day, about three hundred regular donors immediately cancelled their monthly giving. Hundreds of telephone calls had to be fielded by Haloh’s staff. A formal complaint was lodged with the Office of the Privacy Commissioner of Canada by a group of donors.

On her request, the Privacy Commissioner’s office sent to Ruth a huge package, containing privacy checklists and privacy best practices. The key issue for Ruth, however, was to fix the problem. Privacy was considered to be part of risk management. The Privacy Commissioner’s office demanded that Haloh address two major questions: (1) was the company committed to protect the privacy of the donors, and (2) how was this commitment operationalized? Haloh was ordered to analyze and strengthen its privacy practices.
After consulting the management team (see Appendix), Ruth agreed to prepare a report on Haloh’s commitment to privacy. She would hire an outside consultant to conduct an operational audit of Haloh’s privacy practices.

Required:

1.1 What are the requirements for protecting consumer information in your country? Compare these to the ten generally accepted privacy principles (see Andrews and Campbell, 2003 or Parker, 2004). Which principles may Haloh have violated? Justify your response.

1.2 What should be the structure and the objectives for the consulting job? Which professionals could complete these assignments and what standards should they follow? How would Haloh select and evaluate the professional consultants’ work?

PART 2 – COMMITTED TO PRIVACY?

How was Ruth going to answer these questions when Haloh did not have a privacy management program, let alone a risk management program? She had risen through the ranks during the past twenty years and now wondered how the company got into this predicament.

Haloh Foundation, a non-profit corporation registered in the province of Ontario, was founded about forty years ago. Haloh started out as a religious organization building churches around the world. The organization now builds schools and community centers and assists in reconstruction in areas devastated by natural disasters or by war. It also pays for the education of children and for training to create local infrastructure and support. Through five regional centers, funds of over $800 million per year are distributed in over 30 countries. The head office in Toronto employs a staff of 75 in several departments including finance and fund management, program administration, human resources, accounting, marketing, and overseas operations.

The Board of Directors consists of a group of dedicated volunteers. Several directors have been associated with Haloh for many years. Fred, Haloh’s chief executive officer (CEO), particularly relies on the advice of Sam, a retired accountant, and Sheila, a retired lawyer. Both offer suggestions and ideas on a regular basis. Sam also serves on the audit committee which meets regularly to review quarterly financial statements and budgets. The committee approves all office expenditures exceeding $10,000. This committee will have to approve the expected cost of more than $15,000 for the consultants hired to conduct the operational audit. The directors and the audit committee are less involved in overseas operations which are supervised by the vice presidents of the organization (see Appendix).

Jhanna, VP Marketing, and Eric, VP Overseas Operations, hold the most visible portfolios. However, the responsibilities of Sean, VP Finance, and Jan, VP Human Resources (HR), are equally important. The CEO and the VP group hold a formal meeting once a month and meet informally more often if necessary.

Ruth believed a good place to start with her assignment was to get the attention of management. In the past, the company addressed risk management issues at monthly management meetings. It seemed to Ruth that risk management at Haloh was ad hoc – as something came up, it was considered in the context of the entire organization. The topic was only raised again if problems persisted or if implementation questions arose.

Privacy issues had been handled the same way. The Personal Information Protection and Electronic Documents Act (PIPEDA), enacted in Canada in 2000 did not affect Haloh until 2004, as the Act had a staggered implementation schedule. Ruth, in her capacity as the designated Privacy Officer, had drafted privacy policies and procedures. She had compared these with other privacy policies available on the internet. The policies and procedures she had developed had seemed to be adequate, until now.

It appeared to Ruth that demonstrating a commitment to protecting the privacy centered on the following:

- Presence of a privacy culture in the entire organization.
- Senior management involvement, including feedback and approval by the Board of Directors.
- Provision of resources to effectively implement a privacy policy.
- Continuous monitoring and updating of policies and practices.
Ruth placed these items on the agenda for the management committee meeting. During the meeting, her colleagues seemed to be more interested in discovering how the hacking attack had occurred, rather than assisting Ruth in addressing the issue of creating and implementing a new privacy policy.

They agreed, however, that there did not seem to be much of a privacy culture at Haloh. Jan stated that she had not given the privacy issue any attention, because it did not affect her area of responsibility. But now, the Privacy Commissioner’s office had provided a checklist of best practices. One of these practices recommended that all employee files include signed employee privacy statements and that would be clearly the responsibility of HR. Such signed statements did not exist at Haloh. Jan expressed her exasperation at Ruth’s prodding.

“Look, we’ve run with our existing privacy policy for years, and we’ve had little employee turnover – everyone knows what they are supposed to be doing!”

Fred raised his eyebrows and offered the following:

“And those part-time employees? What about them? The point that the Commissioner’s office is making, is that privacy is intended to be organization-wide, and, unfortunately, someone who we can’t identify, put those email addresses on our web site, unprotected. It seems that none of us, and I include myself, really thought that email addresses were all that important! We’ve been focusing on donor addresses and credit card numbers, which, I believe, are more secure. So let’s stop this blame game and just get on with it, shall we? To reduce the costs of the privacy audit, we need to have detailed documentation available about our existing privacy practices. We’ve got this checklist to help us gather the required supporting material. Make sure that the staff in all areas work through it and have the answers ready.”

Fred’s remarks were ignored as Sean explained the effects of the publicity about the phishing.

“The number of donors paying with either check or credit card has not dropped significantly since the security breach. We’ve had about four hundred people move back to the old system of post-dated checks, which means we’ll need staff to deal with that. We called everyone that cancelled the monthly credit card giving, and were able to convince many to change back to the system of post-dated checks. As a result, the number of cancellations from over three hundred has declined to only about two hundred. The overall drop in donations is going to make operations next year a bit tricky though, with higher head office costs. I think you’re going to have to move half of your staff out to the regions, Eric, or face a ten percent budget cut in the coming year.”

Eric grimaced as he thought about the constraints that federal regulations placed upon Haloh’s spending. As a registered charity, Haloh was required to spend a minimum of 80% of its funds to support its operational goals. Haloh aimed for 85%. Spending was always based on the funds raised in the preceding year. A drop in donations meant that head office expenses as well as operational costs had to be cut. The costs for the privacy assessment had to come from operations if donations were down.

Fred turned to Eric.

“Now, I can understand that the current privacy issue has again raised the issue of excess head office costs, but we need to allocate some of the large tasks for the privacy assessment. I’ve briefly reviewed the type of documentation that is required. Let’s look at it by department. This needs to be done without any additional overtime.”

The discussion turned back to what was needed for the privacy assessment.

Jan, in human resources, was to review the job descriptions to ensure that they were current and identify the type of information that employees were allowed to access within the parameters of their jobs. Eric was to do the same for regional operations. There was a new task for him as well – to determine if the operations at remote locations had adhered to existing company privacy policies or if they needed to follow policies that were based on local laws and regulations.

Most of the needed information was to be prepared by the finance and information systems departments, Sean’s area. He was to inventory confidential data at all levels, indicating which job functions should be given access to which information. Then, this was to be cross-checked to the job descriptions. Also needed were information systems tables that provided details about access rights to programs and applications, and how the access rights related to the data inventory. Sean thought that it would be easiest to simply create a list of users and the programs that they accessed. He was not certain if this was possible for all of the application systems.
At first he considered asking for additional resources. But then he reconsidered: Ruth, the controller and second-most senior accounting person, was going to retire next year and Quiang and the other three members of his information systems team, all of them well over 50, seemed to have eased into a low-pressure, good-pay comfort zone. If he was to ask them to do more, he would have to pay them overtime. However, this was not the time to ask for a hiring budget. He and Ruth would just have to do their best.

Ruth summarized what needed to be done. Used to a high level of detail in her work, she was surprised to find that some of the VPs were reluctant to spend time on the privacy assessment. But hen, she did not feel like working all weekend on this report either.

Required:

2.1 Is Haloh demonstrating a commitment to create an acceptable privacy policy? Support your answers. What should be considered when assessing Haloh’s commitment to privacy?
2.2 What documentation should Haloh provide to the consultants for the privacy assessment?

PART 3 – WORKING WITH DONOR INFORMATION

Ruth was not sure anymore about privacy quality at Haloh. It had seemed as if good password practices were in place and that she and Quiang had created a tight safety net for computing. Yet, looking at these reports and the way technology had changed in the last few years, she was getting confused. She was looking forward to working with the consultant to resolve her questions, but dreaded the possibility that there just might be one or two major problems that had to be fixed. Ruth had accumulated a pile of papers, close to six inches thick, for the consultant. The operational audit of privacy practices over donor information was a bit of a challenge.

Haloh hired the firm of Gregory, Ng and Chu, LLP, a medium-sized accounting firm, to conduct the donor information operational audit. Frank, an experienced professional at the accounting firm, was assigned to work with Haloh. Frank had obtained background information about Haloh when his firm discussed the engagement (see Table 1). Frank commented to Ruth that the Haloh policies were quite general and did not address specific business processes. Frank asked for more specific information about access levels and methods of setting and maintaining access rights than what Ruth had supplied (see Tables 2 and 3, respectively).

TABLE 1 – BACKGROUND INFORMATION: DOCUMENTS PROVIDED FOR DONOR INFORMATION OPERATIONAL AUDIT

<table>
<thead>
<tr>
<th>Document title</th>
<th>Purpose and details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee information systems access policy</td>
<td><strong>Purpose:</strong> Limit access to information and functions on a need-to-know basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Details:</strong> Provides methods for authorizing users, states that each employee</td>
</tr>
<tr>
<td></td>
<td>is to have a unique identification code and password. When employees leave</td>
</tr>
<tr>
<td></td>
<td>Haloh, their identification codes are to be deactivated.</td>
</tr>
<tr>
<td>Employee code of conduct</td>
<td><strong>Purpose:</strong> Address software ownership and ownership of Haloh data.</td>
</tr>
<tr>
<td></td>
<td><strong>Details:</strong> Software rights belong to Haloh; no unauthorized software is to be</td>
</tr>
<tr>
<td></td>
<td>loaded onto Haloh systems. Haloh data is to be treated as confidential.</td>
</tr>
<tr>
<td>Web site privacy code</td>
<td><strong>Purpose:</strong> Inform donors and potential donors of Haloh’s privacy policies.</td>
</tr>
<tr>
<td></td>
<td><strong>Details:</strong> Basic disclaimer, stating that Haloh uses donor information internally,</td>
</tr>
<tr>
<td></td>
<td>does not sell to or share donor information with third parties, and does not</td>
</tr>
<tr>
<td></td>
<td>post credit card information on its web site.</td>
</tr>
<tr>
<td>Contract with credit card payment processing</td>
<td><strong>Purpose:</strong> Identify responsibilities of Haloh and the service provider.</td>
</tr>
<tr>
<td>provider</td>
<td><strong>Details:</strong> Credit card provider is solely responsible for processing payments</td>
</tr>
<tr>
<td></td>
<td>and refunds, and will retain donor information on its systems no longer than</td>
</tr>
<tr>
<td></td>
<td>six months.</td>
</tr>
</tbody>
</table>
Data retention policy

**Purpose:** Describe backup processes, and indicate the length of time that Haloh data is retained.

**Details:** Backup files kept on site, and a copy is kept at the local bank. Data is to be kept only as needed for administrative, accounting, or marketing purposes.

Table 2 shows that there are three different sets of access rights: first, the overall access to the local area network, second, separate access to the accounting systems, and third, separate access to the operational database management systems. The latter consists of (1) a donation reporting system used to track donations received, and to issue receipts and (2) a donations receivable system for tracking and monitoring pledges.

**TABLE 2 – ACCESS LEVEL DETAILS**

<table>
<thead>
<tr>
<th>System level</th>
<th>Access available at that level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local area network</td>
<td>Office automation software (Word, Excel, PowerPoint, Internet Explorer), Intranet containing documents that all employees need access to, including donor email file, utilities to upload information to the web site</td>
</tr>
<tr>
<td>Accounting systems and donation reporting</td>
<td>Accounting software packages including general ledger, accounts payable, payroll. Customized software used for tracking donations, donation reporting and sending donation receipts.</td>
</tr>
<tr>
<td>Operational database management systems</td>
<td>Proprietary project management software for regions, client management system.</td>
</tr>
</tbody>
</table>

Ruth designed an email form on which Jan checks the box indicating which area the person works in. The form then moves through the various departments as follows:

- The employee supervisor lists the functions the employee is to have access to, by checking boxes and adding functions not listed. S/he then forwards the form to Ruth for review.
- Ruth checks the access levels required, and forwards the form to the appropriate person for establishing access, as follows:
  1. Ramin, the Accounts Payable Supervisor, for accounting system or donation reporting access.
  2. Geoff, the Senior Analyst, for local area network and operational database access.

When UserIDs (user identification codes) and initial passwords have been established, using the protocols described in Table 3, both Ramin and Geoff type the authorization email, print it, sign it, and forward the signed document to human resources for filing in the individual's human resources file.

As an additional safeguard, neither Ramin nor Geoff can ‘refresh’ an employee’s memory in case s/he forgets the password. They can reset the password to “iforgot.” The passwords are to be changed immediately after an employee’s first sign-in with the “iforgot” password. Marketing personnel have access to the donation reporting system, while accounting personnel have access to both donation reporting and donations receivable.

Employees in overseas branches do not have access to the donation and accounting systems. They have access to operational database management systems.
### TABLE 3 – ACCESS RIGHTS

<table>
<thead>
<tr>
<th>System Level</th>
<th>Initial Access Process</th>
<th>Follow-up Access Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local area network</td>
<td>Determine a new UserID code; inform accounts payable supervisor of new UserID code; set initial password to ‘imnew.’</td>
<td>Block employee access by changing password to a random string if new password is not enacted within two business days of hire. If a user forgets the password, reset to ‘iforgot.’</td>
</tr>
<tr>
<td>Accounting systems and donation reporting</td>
<td>Set up a ‘new user’ access code using the UserID created earlier and set the initial password to ‘imnew’ to provide access to the accounting or donation reporting systems.</td>
<td>Block employee access by changing password to a random string if new password is not changed by the end of the first day of employment. If a user forgets the password, reset to ‘iforgot.’</td>
</tr>
<tr>
<td>Operational database management systems</td>
<td>Set up ‘new user’ access code, as above.</td>
<td>As above.</td>
</tr>
</tbody>
</table>

From access rights and setup, the discussion between Ruth and Frank moved to an analysis of existing users. They worked with a report of user identification codes for the local area network and for the accounting system. The accounting system had 77 users, and the local area network had 476 users. It was not possible to determine from the local area network list any employee’s department, so Frank gave the list to Jan and asked her to find the information. The review by Jan revealed that:

- The access codes to the accounting system of two employees who did not return from maternity leaves had not been removed from the system;
- Six employees with access codes to the operational database management systems had two UserIDs, although the duplicate UserIDs were not in use; and
- The access codes of former part-time staff that prepared and mailed donation receipts three months earlier had not been removed from the system.

Before meeting again with Frank, Ruth asked Quiang to immediately delete the obsolete UserIDs.

Next, Frank turned his attention to internet donation and recording of donor payment information.

> “You’ve told me that credit card donations are received via the web site using a third party provider. The payment, less commission, is deposited directly into Haloh's bank account. As transactions are processed, the credit card service provider sends payment details (including the donor’s name and address) to Haloh. The payment details are entered into the donation reporting system and, using a Word document template, a donor receipt (Pdf file) is created.”

Ruth nodded, looking a bit depressed. Without success, she had tried to change to a Pdf-based reporting and receipt generating system. Instead of investing $5,000 on new programming that would have increased efficiency and productivity for many years, the company decided to spend only $2,500 on error-prone, part-time help, hired at minimum wages.

Everyone, including Ruth, had expected that existing personnel would be able to prepare the Pdf documents by cutting and pasting each name and address into a Word document. They had expected only three or four hundred receipts which could have readily been handled by full-time staff. However, marketing had done a superb job, and several thousand donations came in from the December Telethon, mostly in small amounts of less than $25. This meant that the work was too much for existing staff, resulting in the need to hire the part-time help.

Ruth confirmed that the Word template was on the intranet. All employees had access to and retrieved the template from the intranet to prepare the Pdf donor receipts, everyone except management and information systems personnel. The completed word documents used to generate Pdf donor receipts were saved alphabetically by last name on the intranet, with one folder for each city within each province. The files were saved using a filename that consisted of the donor’s last name, first name and donation date to create unique file names. Pdf files were generated and saved in the same folder as the original.
Word document. Ruth was comfortable with the level of security that had been established, as only employees had access to the intranet. Frank’s next question about donors surprised her, however.

“Who is responsible for reconciling donor information on the web site and the donation reporting system?”

Ruth stared at him.

“Reconciling the web site? There’s no financial information there. We reconcile the information from the credit card provider to the donation reporting system, to make sure that we have sent tax receipts for everyone who made a donation.”

From his seemingly bottomless briefcase, Frank pulled several donor summary reports that Ruth had given him previously.

“OK, you’ve had this web site for about five years, but it is only in the last few months that you have sent Pdf donation receipts. Before then, you entered the information into the donation system and had receipts printed from there, which were mailed. Last year, you had donations from 111,246 donors. There are just under 463,000 donors listed in the donation system, and there are just under 235,000 donors listed on the web site. This should mean that you have had 235,000 online donors in the last five years. The question becomes, when was the last time that these people made a donation, and how long are you going to keep their information?”

Now, Ruth understood what he was talking about – one of the principles associated with privacy was keeping information only as long as one had a need for it.

She was on familiar ground – she had had this discussion frequently in the past. Usually she was the one trying to get others, specifically marketing, to agree to delete some old donor information, primarily to free up computing capacity.

“Marketing likes to keep the information for at least ten years. Depending on our budget, we send rotating mail promotions to different letters of the alphabet, with a selection of the older accounts included. You’d be surprised at the number of long-time absent donors who send in money.”

Frank then returned to access rights.

“What about the information systems staff? What do they have access to?”

Ruth paused for a moment, and rather than being evasive, she came right out with it.

“They have access to everything, as they do maintenance and install upgrades to our software, including the security systems. They’re all super users.”

Frank nodded and thought to himself that it was typical for a small information technology group to function that way.

Required:

3.1 Identify the strong features of the present donor information system and explain the benefits to data privacy at Haloh.

3.2 Assume that you are Frank, the consultant. Prepare a draft of a management letter to Haloh management. Use the following tabular method for your management letter: clearly state the potential privacy management weakness (W), the impact of the weakness (I), and a recommendation (R) for improvement. List additional areas or questions (Q) that need to be reviewed or answered.

3.3 Describe how Haloh should implement a coherent privacy policy and privacy practices. Be specific.

APPENDIX – CAST OF CHARACTERS

<table>
<thead>
<tr>
<th>Board of Directors and Executive Management</th>
<th>Other listed employees, reporting to Executive Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of Directors</td>
<td></td>
</tr>
<tr>
<td>Sam - retired accountant, also on audit committee</td>
<td></td>
</tr>
<tr>
<td>Sheila - retired lawyer</td>
<td></td>
</tr>
</tbody>
</table>
**Executive Management**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fred</td>
<td>Chief Executive Officer</td>
</tr>
<tr>
<td>Sean</td>
<td>Vice President Finance</td>
</tr>
<tr>
<td>Ruth</td>
<td>Corporate Controller, Ramin</td>
</tr>
<tr>
<td>Quiang</td>
<td>Information Systems Manager</td>
</tr>
<tr>
<td>Geoff</td>
<td>Senior Analyst</td>
</tr>
<tr>
<td>Jan</td>
<td>Vice President Human Resources</td>
</tr>
<tr>
<td>Jhanna</td>
<td>Vice President Marketing</td>
</tr>
<tr>
<td>Eric</td>
<td>Vice President, Overseas Operations</td>
</tr>
</tbody>
</table>

**ACKNOWLEDGMENTS**

The author gratefully acknowledges receiving access to use the resources of the November 2006 Case Writing Workshop sponsored by the Toronto Chapter of ISACA (Information Systems Audit and Control Association) and the University of Waterloo, Centre for Information Systems Assurance. Thank you also to the anonymous reviewers and to Cristobal Sanchez-Rodriguez, York University for their helpful comments.

**REFERENCES**
