

### **Introduction: Setting the Scene**

The prompt for this exercise proposes a scenario where there has been a breach in information privacy. An employee has downloaded and sold large sets of confidential customer data to others outside the organization. This data is used within the organization to develop business intelligence. Given my current status as a doctoral student in FSU's College of Communication of Information, I have chosen to apply this scenario within the confines of the College. I will take the large set of data to be a database (which as far as I am aware does actually exist) of all current students and past alumni, data that clearly is used by the College to generate intelligence both on current students and alumni. If I was in a managerial role within the College, I would respond to this crisis first by quickly identifying the important factors to consider, then by taking action to inform students and alumni, discipline the employee, and ensure the organization learns by changing data and knowledge management practices to increase the level of privacy protection for students and alumni.

### **Factors to Consider**

Numerous factors would need consideration when deciding upon the appropriate actions to take in response to the data breach. Chief amongst these would be to determine what specific data on the students and alumni was compromised. In this case, the College's database contains (as far as I am aware) names, addresses, phone numbers, e-mail addresses, courses taken (without grades), FSUIDs, and—as the primary key—students' FSU security numbers (FSUSNs). Another important factor is determining how sensitive a breach of this data would be. Given these specifics, an outsider would have access to personally identifiable information that links students and alumni to where they live, how they can be reached, and what courses they have taken. Perhaps most critically, they would have the FSUSN and FSUID for each student and alumnus, and thus would be able to look up even more private information via FSU's Blackboard and Secure Apps systems. This data could also be used for profiling, as noted by Smith (2004b, pp. 212-213). This breach, therefore, would require an urgent response.

Other factors worth consideration stem from Smith's (2004b) discussion of managerial action areas for information privacy. Alongside profiling, the most critical of these would be secondary use, data accuracy, and authorized access. The breach, as an unplanned and unauthorized secondary use, would likely present legal liabilities for the College and for FSU. Smith suggested examining "internal secondary uses" to lessen the potential liability and risk (p. 208). The accuracy of the data would also be an important factor; if the list of courses was incorrect for a student or alumnus, for example, an employer who happened across the compromised data might incorrectly conclude that they did not take a course they claimed to, potentially leading to unwarranted disciplinary action. In this case Smith suggested allowing the students and alumni to correct their own data (p. 209); the organization then would need to ensure this corrected data made it into the database as soon as possible. Finally, authorized access would clearly be one of the most important factors in this case. The employee who sold the data to those outside the organization may or may not have had authorization to use it as part of his or her job responsibilities, and potentially may have been able to download the data, but would certainly not have been allowed to release it to the outside world. Smith (2004b) argued for "restricting access to the smallest possible data unit" (p. 210), which would help reduce the

scope of the data the employee had access to and / or could download. It would also be important to identify whether the employee used his or her own account to download the data or “borrowed” another employee’s account.

### **Specific Actions**

Given the severity of the breach, it would probably not be wise to take the time to carefully follow Smith (2004a)’s “steps to take when [ethical] quandaries arise” (p. 114); while these certainly provide good advice, the situation would simply be too critical to spend much time on a full analysis. At least one action would need to take place immediately, in my view: informing students and alumni of the incident and that FSU and the College are doing everything to resolve the situation. This would let the most important stakeholder know the situation; unfortunately it would be impossible to let all stakeholders know—as argued for by the stakeholder perspective Smith (2004a) presented—without widely publicizing the breach, inviting bad press that may damage the College and university’s reputations. Another action I would take immediately would be to shut off all access to the account of the employee suspected of downloading the data. If they admit to the breach, I would apply appropriate disciplinary action, most likely removing them from their position given the severity of the situation. If they claim they did not download the data or that someone else used their account to do so, an investigation would be necessary to determine to whom the evidence points most strongly. These actions would cover the factors of the severity of the breach, the specifics of the data released, and the potential for profiling.

Other factors would provide ample opportunities for organizational learning. As noted above, Smith (2004b) argued for lessening internal secondary uses; these could be reduced by providing more barriers to the downloading and sharing of data within the organization. I would thus ask the IT staff to implement security controls for the downloading feature, limiting its use to the highest levels only. This would also tie into authorized access: I would further ask IT to implement restrictions on the specific fields employees can access, as suggested by Smith. This would restrict the access of those sending out mailings, for example, to only the names and mailing addresses, keeping other data from being accessed or downloaded. Since employees might commonly perform multiple tasks, each needing different privileges, I would also consider—if in agreement with other managers and staff—asking IT to create separate accounts for each task, which employees could then log in and out of as necessary. Next, although FSU already allows students to correct their own name, mailing address, phone number, and e-mail address through Secure Apps, I would ensure that the College picks up on these changes as soon as is technically possible. I would also give students who are about to graduate the opportunity to check the accuracy of the list of courses they have taken, as part of graduation check procedures. Finally, if it was not already required I would ensure all employees took part in privacy and ethics training, to ensure they are aware of university, state, and federal laws, regulations, and policies regarding data and knowledge about students and alumni.

### References

- Smith, H. J. (2004a). "But what is the 'right thing'?": Ethics and information systems in the corporate domain. *MIS Quarterly Executive*, 3(2), 105-115.
- Smith, H. J. (2004b). Information privacy and its management. *MIS Quarterly Executive*, 3(4), 201-213.