Disaster at a University – A Case Study

Turn Key University (TKU) is a medium sized public university located in Idaho. The institution is situated on a beautiful 25 acre campus, just north of a major city. The University consists of over 6,000 students mostly from the surrounding region. The institution is a liberal arts college that offers over 30 undergraduate majors and a dozen graduate degrees. The school has a reputation for producing quality graduates for the surrounding community. The University is a major employer in the area, providing jobs for over 900 employees.

Organization Hierarchy

The institution was organized as a typical university bureaucracy, with the President's office overseeing the Academic Affairs, Administrative Support Services, Human Resources, Finance, and Information Technology divisions as shown in Figure 1. The IT, Finance, and Administrative Support divisions are the primary focus of this case.

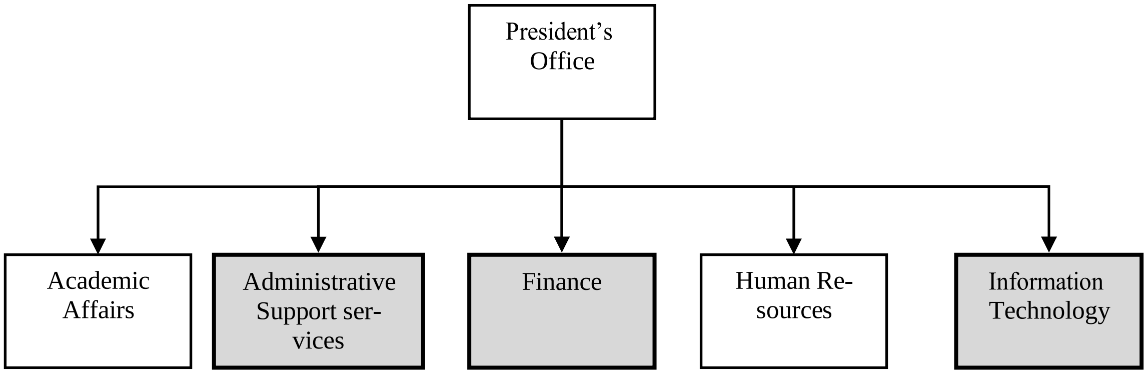

Figure 1: TKU's Organizational Hierarchy

As shown in Figure 2, the Information Technology division consisted of six departments -- Institutional Projects, Media Services, Teaching Support, Computing Systems, Web Services, and Network & Telecom. Each of these departments was managed by a Director who reported to the Chief Information Officer (CIO). The Information Technology Division managed all aspects of computing on the University campus. The IT division employed over 70 permanent members and several temporary/student employees. The IT division required a large server farm to manage a transaction management system and other systems. TKU centralized all server functions in the Computing Systems department.

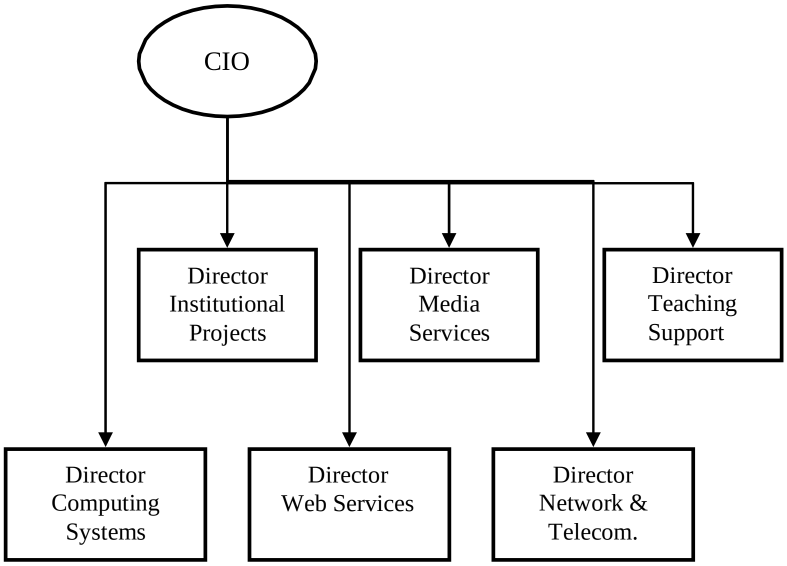
CIO
Director Institutional Projects
Director Media Services
Director Teaching Support
Director Computing Systems
Director Web Services
Director Network & Telecom.

Figure 2: IT Division Hierarchy

Administrative Support Services supported the ancillary services offered by the college. Among other things, this division managed relationships between the on-campus and off-campus vendors. On-campus vendors include the post office, GoodFood (the student meal plan provider), CollegeBooks (the bookstore operator), and FastSnack (the snack machine provider). The snack machines were an important part of students' life as many students relied on late night RedBull® runs to make it through a last minute cram session. Off-campus vendors include restaurants, tanning parlors, and gas stations. Compared to the IT division, Administrative Support Services was relatively small, with approximately one-fifth the numbers of personnel in the IT division.

The Finance Division was responsible for managing and reporting the financial state of the University. The division was made up of five departments: Financial Affairs, the Budget Office, Accounts Receivable, Accounts Payable, and Student Services. All financial information reporting was overseen by the Financial Affairs department. Overall, the Finance division employed 30 permanent employees and several part-time members on a need basis.

System Description

Since 2000, TKU used a transaction management system for student meal plans. There were three different meal plan tiers: a lower volume plan that was aimed towards commuters, a middle volume plan that was targeted for full time students who leave on the weekends, and a high volume plan that was designed for students who eat all meals on campus. Out of the three plans, the middle volume plan was the most popular among students and responsible for the majority share of the transactions.

In addition to the meal plans, the transaction management system handled virtual dollars. Virtual dollars can be thought of as a prepaid credit card. At the beginning of the semester students were given a balance based on their meal plan, and students drew down the balance by purchasing items from vendors. Students and parents were also able to add additional funds on the card through an online portal. Students paid for items using virtual dollars at a variety of vendors – they spent it on books from the bookstore, stamps from the post office, drinks from the snack machines, and on food from neighborhood restaurants. Virtual dollars were a hit with students as they enjoyed having the freedom and convenience to pick what they wanted, when they wanted.

The transaction management system was more than a way for students to purchase food; it was also a profit center for the college. From a fiscal perspective, the system was able to generate annual profits of $600,000 for TKU. Most of the revenues were from commissions on sales to vendors. Due to corporate cultural issues (as discussed below), the control of the system spanned across the IT, Administrative Support Services, and Finance divisions, although none of the divisions received commissions. All the money generated from the system went into a central fund managed by the President's Office.

History of the System: Reflection of Corporate Culture

The Transaction Management System (TMS) had been in place for over ten years at the writing of this case and within that time frame it had changed hands multiple times. Initially the system was handled by the Computing Systems department in the Information Technology Division. The typical system administrator learned about the system on-the-job in an informal fashion, and there was a lack of process or steps that could be reproduced when system administrators changed. Further, when the system was implemented, security was an afterthought and security responsibilities played a minor role in system administrators' job duties. As a result, the current state of the system was that (1) there was a lack of formal process in managing the system and (2) the system was never secured. At the time of writing, the system was managed by two administrators – Gary and Tom from the Computing Systems department. They had been in their roles for a little over a year.

Although the TMS system depended on multiple divisions (IT, Finance, etc.,) for effective operation, the incentives in place were conducive to reinforcing the functional boundaries among various divisions (see Figure 1), thus resulting in friction among divisions. As the TMS grew in stature, the logical solution to reduce the political tensions among divisions was to split the system responsibilities among the divisions. In this arrangement, IT continued to manage the servers with Gary as the primary administrator and Tom as the backup. The Finance division took over the administration and user access portion of the system. The responsibilities for system administrator fell on Don who had some technical background and was seen as a 'tech geek' in the Finance division. At the time of this case study, Don had been in the system administrator role for three months. When Don inherited the system, he received no formal system administration or security training and found that there were no formal policies or business rules in place. As he learned the system, he realized it housed a large amount of personally identifiable information (PII). There were student social security numbers (which acted as a students' primary ID in the university system), addresses, phone numbers, birthdates and meal plan information.

The Security Structure: Technical Safeguards

The security structure was handled in two different ways. The first was by ensuring only authorized people had access to the system. The second was by viewing events in the log files. The system was set up in a typical hierarchical structure, comparable to Windows Active Directory.
There were user accounts that branched into user groups. People could access the system by logging in with a username and password, similar to how a person would access their home computer. When a user needed an account, the system administrator would assign a username and password. Once a user had a username, the system administrator placed the user in the appropriate user group, which determined what functions the user could perform. The administrator group had full permissions and consequently had free reign of the system. Among other things, the administrator could run reports, change meal plan settings, upload data and export data from the system.

The next method of managing system security was through the log files. The transaction management system created system logs whenever an event occurred. This feature was very useful for showing what happened within a system. The logging feature showed the time, the user group, and the event that occurred. While the logs were useful, the primary drawback was that they only showed what group created an event. As a result, events could only be seen at the group level.

This means if a user logged into the system and made a change and was a member of the administrator group, the log would only show that someone in that group made a change. It didn't show which user made the change.

The Issue: Data Breach

Early one morning, Don was ushered into a closed door meeting with the Chief Finance Officer, the CIO, and an external security auditor he hadn't met before. In the meeting Don learned that large amount of data, including the PII, was exported from the system. The previous day Gary was going through the logs to see if the patch he applied worked correctly, and he noticed that someone in the administrator group had exported a large amount of data at an odd time. Gary rea- soned that no one should be accessing the system at 2am, and he was concerned because a large amount of data was exported. After bringing up the issue to management, it was decided that the Finance division would investigate the issue. Therefore, the responsibility to figure out exactly what happened fell on Don. He was asked to work with an auditor to find out exactly what hap- pened. Don left the meeting feeling overwhelmed and disconcerted; he knew nothing about secu- rity practices and he wasn't happy about working with the auditor. He had recently inherited the system and didn't know much about it. He did know that he had to find the source of the leak be- fore more student information was lost and he knew his job might be on the line.

The Investigation: Lax Security Policies and Culture

The auditor decided to interview the users of each business unit. At a basic level, he wanted to figure out if the leak was an internal job or if TKU had fallen victim to a hacker. So, he wanted to see the different entry points that a potential hacker could get access to the system. Further, the auditor felt it necessary to check the user account structure, the business rules, and department norms. By doing this, the auditor felt confident that he could determine which user in the administrator group was responsible for the data leak, if it was an internal job. Throughout the investigation, Don was going to support the auditor and would provide the required information.

The auditor and Don started the audit process by going through the system. They checked the user accounts and found multiple points where a hacker could have entered the system. They found over 50 orphan accounts, which are accounts that had been set up but never used. When an account is set up, the policy is for the system administrator to provide the same generic password. Once a user logs into the system, they are prompted to enter a new password. Since none of these accounts were used, all of the accounts had the same password. A hacker could have easily cracked the generic password and gotten access to the system.

Another area of concern was with password complexity. The system didn't require users to have strong passwords. Passwords could be as short as three characters long and didn't need to include numbers or special characters. The passwords could be kept forever and most had never been changed. With the current sophisticated password cracking programs available on the Internet, hackers could break into the system in seconds. This seemed very likely as figuring out the system usernames was very easy. The usernames were based on the name of the user. The first letter of the username was the first letter of the person's first name. The last part of the username was the person's last name. For example, Gary Tolman's username was gtolman. This type of username assignment is very common, but it can also pose a threat. Each employee's name was listed on the TKU website, so a hacker could easily find a username.

Lastly, the system was accessed by a variety of users. They were spread out between Information Technology, Finance, and the Administrative Support Divisions, so finding the exact users would be difficult. Anyone in these divisions could be the source of the leak. Don and the auditor didn't know how they were going to trace the culprit, but they knew they had a daunting task. They started off by interviewing people in the three divisions. The Administrative Support Services division used the transaction system to run reports, so the users only had permissions to run re- ports. Don and the auditor found that in addition to the approved users, more people accessed the system. Employees routinely gave out their login information to student workers and temporary employees to run reports when they were busy or on vacation. The employees shared this login information on Post-it® notes, over the phone, and in email. The department did not have rules explaining proper procedures, so employees thought these practices were acceptable and the norm.

Next, Don and the auditor interviewed people in the IT Division. They focused on the Computing Systems department, which handles the technical end of the transaction management system. This includes duties such as managing the server, setting up off-campus merchants, maintaining on-campus connections, and troubleshooting networking issues. The transaction management system from an IT perspective is a server with a simple front end that users log into and a database that holds the information. Don and the auditor found that there were no formalized policies or procedures detailing how to complete tasks. There were no business rules and the department lacked consistency in its approach to managing the system. In this department, three administrators had full administrative rights, so they had full access to the system, allowing them to add user permissions or initiate data exports. During the interview, Don and the auditor also realized that in the past when IT handled information security employees routinely gave out initial passwords in email or on the phone. There was only one clear written policy and that was broken routinely.

The policy stipulated the Finance division was to extract the required data to run reports from the system. However, the IT division continued to extract data for the majority of users. People preferred IT to extract the data because they were quicker than Finance. Further, the auditor was informed that there was a major upgrade to the campus infrastructure recently, and during that time outside contractors were on-site as technical advisors. The contractors were supposed to have given limited access, but by this point, the auditor was not convinced if this exactly happened.

The following day, Don and the auditor looked at the Finance division. The Finance division handled the system administration and the access permissions for the system. The department also oversaw the functional components, such as crediting accounts if a student was charged incorrectly for an item. The system was also used to run business intelligence reports. Don was the primary administrator for the system, so he had complete access to it. He was able to perform functions such as setting up user accounts and exporting data. It was his responsibility to ensure that correct people had access to the system.

At this point, Don took a back seat and the auditor interviewed him. The auditor realized that Don didn't have much experience managing the system. Further, he also gave out passwords to users through email or on the phone. The auditor also found that Don didn't require users to have strong passwords. Next, the auditor interviewed the accountants that used the system. The ac- countants had only limited access to the system. They could post transactions and transfer funds, but nothing to the extent of exporting data.

The Outcome: Victim of Social Engineering

Throughout the process, the auditor found countless examples of lax information security throughout the organization. There was a lack of a coordinated security policy, and the policies in place were not being followed. While reviewing the notes, the auditor noticed that a contractor requested the TMS server address over the phone. Further follow up revealed that a system administrator gave out the server address to a contractor because the contractors were in the middle of upgrading servers. The administrator also mentioned that the contractor requested the pass- word, but the administrator didn't feel comfortable sharing the password on the phone and asked the contractor to stop by the office – but the contractor was a no show. From the description of the events, the auditor felt it was a social engineering attempt. Social engineering is when a hack- er attempts to gain access to sensitive information by tricking a person into giving it to them. The immediate recommendation of the auditor was to focus on the contractor's activity in the organi- zation.

Over the next few weeks the story unfolded and all the pieces of the puzzle were put together. It was eventually proven that the contractor stole the information. The contractor was hired to over- see the upgrade of servers on the storage network. While doing this, she learned about the trans- action management system. She knew PII could be sold on the black market and thought the lax security at TKU would enable her to get away with stealing data without any repercussions. Her only obstacle was access. Since she only had access to the storage network, she needed a way to get access to the transaction management server. That's when she called the system administrator and got the IP address and tried to get his login credentials. Once she got the IP address, she was able to utilize the free tools available on the Internet to scan the system and get the username and password with administrative access. It took her only a matter of minutes to get this information. The password was only three characters long and didn't use any numbers or special characters.
With her new administrative permissions, she was able to export the PII.

The Aftermath

TKU was very lucky with the outcome of the data breach. Only five hundred students had their information compromised. While any loss of PII is unfortunate, high profile data breaches, such as the ones at TJX, show how losing large amounts of data can be very costly to an institution. Like many businesses, the University attempted to keep the data breach quiet, but the breach in- formation was eventually released. The fear of student backlash and the need to be compliant with privacy breach laws forced the university to inform the campus community of the breach. Students were initially very angry and felt as though they could not trust the university with their private data. To help improve student morale, the president offered reduced tuition for a semester and a year of paid credit monitoring service to victims of data breach. The University's generous response helped to calm the protests, but it came at a price. TKU estimated that the tangible costs associated with the breach amounted to over $600,000 dollars. However, TKU will never know how the breach affected the university's reputation.