Journal of Information Technology Teaching Cases (2011) 1, 40–49
© 2011 JITTC Palgrave Macmillan All rights reserved 2043-8869/11
palgrave-journals.com/jittc/

Teaching case

Addressing the new regulatory landscape: IT compliance and E-Discovery at KMCO Gaming

Christina N Outlay[1], Poornima Krishnan[2], Chandrasekaran Ranganathan[2]

[1]DePaul University, Chicago, IL, USA;
[2]University of Illinois Chicago, Chicago, IL, USA

Correspondence:
CN Outlay, DePaul University, 1 East Jackson Boulevard (MC 6000), Chicago, IL 60604, USA.
Tel: +1 312 362 6965

Abstract

With the advent of federal regulations such as the Sarbanes Oxley act and the amended Federal Rules for Civil Procedure guidelines, KMCO Gaming, a leading manufacturer of casino gaming systems, is grappling with managing electronic data and records in compliance with legal requirements. In the midst of a major lawsuit against a rival company, KMCO has decided to purchase an electronic discovery (E-Discovery) solution. E-Discovery is the process of finding and producing digital information needed as evidence for legal matters. To implement such a solution, KMCO would need to develop a formal governance structure, processes for electronic file storage and sharing, and technology tools to support the new E-Discovery system. This case provides an overview of the regulatory landscape that impacts management of electronic records and highlights some of the organizational challenges that may impede the ability for IT management to successfully deliver IT compliance initiatives. Names and identifying facts related to the company, key players and key events described in the case have been changed.

Journal of Information Technology Teaching Cases (2011) **1,** 40–49. doi:10.1057/jittc.2011.1; published online 8 February 2011

Keywords: E-Discovery; document classification and management; enterprise data management; IS policy; IT compliance

Introduction

Bruce Isaac, Executive Vice-President of Information Technology of KMCO Gaming, sat in his office pondering what their next steps should be. KMCO had recently lost a lawsuit against its rival BJH due to KMCO's inability to convince the courts that its computer procedures were standard, legally defensible, and that its data was forensically protected. For the last 2 years, KMCO had been implementing its electronic discovery (E-Discovery) project to deal with several United States legal compliance requirements for electronic document storage and retrieval. Judging by this recent court loss, the E-Discovery project was not yielding the expected results, which would now delay KMCO's plans to implement additional changes. Worse, with the lawsuit verdict going against them, Bruce wondered whether KMCO's Chief Financial Officer (CFO) and Chief Executive Officer were going to continue funding the project at all.

As Bruce worried about KMCO's E-Discovery project heading towards a complete failure, he wondered what had gone wrong, who was responsible, and most importantly, what to do next. The KMCO Legal Department staff was blaming the Information Technology (IT) group for the project failure, while IT was pointing fingers at Legal, so identifying who was responsible was just as difficult as identifying what went wrong. As far as next steps, there were two options: Bruce could lobby for continuing the E-Discovery project as planned and chalk up the lawsuit loss as an occupational hazard. Or, he could stop the project and hire outside consultants to recommend a new strategy and implementation plan.

KMCO gaming – background

Company description

KMCO Gaming was a pioneer in designing and manufacturing gaming systems. Formed originally in the 1950s as a distributor of pinball machines, KMCO later expanded its operations to include home video entertainment, casino gaming and other state-of-the-art electronic entertainment systems. By the time they were incorporated in 1975, KMCO decided to focus on casino gaming systems and became publicly traded on the New York Stock Exchange (NYSE) in 1983.

KMCO quickly distinguished itself as a leader in casino gaming design and development. They continuously invested in cutting-edge technologies in order to improve their existing product offerings, while simultaneously developing innovative new products that appealed to gaming enthusiasts. By 2008, they had a strong market presence in the gaming industry, a reputation for innovative game design and development, and total revenues of over $700 million. The majority of this revenue was generated through sales of their video and mechanical gaming systems (Table 1), which they sold to casinos, hotels and resorts. Beyond sales of their gaming systems, KMCO generated additional revenues from operating and maintaining these gaming systems for their current customers.

KMCO was based in St. Louis, Missouri and for over 20 years following their initial public offering, their primary clientele consisted of casinos throughout the United States, US Territories and Canada. Business was steadily growing; the increase in visitors to North American destinations such as Las Vegas and Atlantic City continued to increase for both KMCO and other big players in the industry. With the addition of new gaming territories in North America, KMCO was expected to grow substantially at the end of year 2001.

Buoyed by their success in North America, KMCO began expanding their reach globally. From 2006 to 2008, KMCO acquired Gaming Strategists, Inc. (GSI), an international distributor of gaming machines and services based in Japan and Germany-based RBT Systems. The acquisitions gave KMCO immediate entry into the international gaming market, and KMCO quickly set up additional offices in France, Italy, Australia, South Africa and South America. By the end of 2008, KMCO's international sales represented 75% of the firm's total earnings.

Table 1 KMCO – revenue streams

Product line	*Year*		
	2008 (%)	*2007 (%)*	*2006 (%)*
Video game machines	48.60	49.70	48.40
Mechanical reel game machines	18.90	15.80	7.00
Video poker game machines	0.10	0.90	1.90
Other products	32.40	33.60	42.70

By 2008, the gaming industry focus had gradually moved from mechanical gaming systems to server-based gaming systems. Traditional mechanical gaming systems (also called slot machines) are standalone machines that are often custom-built to offer one type of game and have mechanical reels that determine the outcome of the game (see Appendix A). Server-based gaming systems (Appendix B) are connected to central servers that collect data from all machines in an arcade or casino, can offer multiple games from one machine, and contain a microchip that determines the outcome of the game. Server-based gaming systems would offer casinos and arcades the flexibility to change games without changing machines. Moreover, the data collected from all machines could be used to identify and market to specific customer profiles.

The gaming industry's emphasis on server-based systems meant KMCO could expect their 'Other products' revenue stream to begin growing faster than their Video and Mechanical gaming streams. KMCO (and its competitors) were investing resources and considerable R&D effort into developing gaming content and technology for their server-based gaming offerings. KMCO was certain it had blockbuster game concepts for the coming wave of server-based gaming and was eager to be the first company to introduce a full-featured server-based game system to the market.

KMCO's company structure

By 2009, KMCO had nine international offices servicing 28 countries, 15 regional offices servicing the United States, Caribbean and Latin America, and two research and development subsidiaries, in addition to their Corporate Headquarters offices in Missouri. The company was divided into four divisions (Figure 1): Innovation and Product Development, led by Ralph Danes, was responsible for research and development (R&D) at KMCO. R&D was the

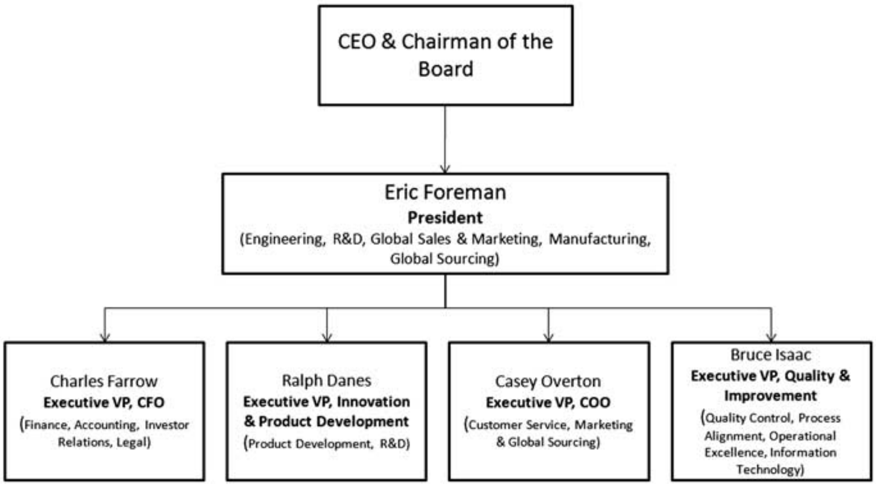
CEO & Chairman of the Board
Eric Foreman
President
(Engineering, R&D, Global Sales & Marketing, Manufacturing, Global Sourcing)
Charles Farrow
Executive VP, CFO
(Finance, Accounting, Investor Relations, Legal)
Ralph Danes
Executive VP, Innovation & Product Development
(Product Development, R&D)
Casey Overton
Executive VP, COO
(Customer Service, Marketing & Global Sourcing)
Bruce Isaac
Executive VP, Quality & Improvement
(Quality Control, Process Alignment, Operational Excellence, Information Technology)

Figure 1 KMCO – org chart.

oldest division in the firm, responsible for the blockbuster game system prototypes, and was held in the highest esteem throughout the organization. Ralph Danes had worked with the founder of the firm since the firm's inception and had a personal friendship with the Board chairman. The customer service, manufacturing, sourcing and global supply chain management division, led by Chief Operating Officer (COO) Casey Overton, managed KMCO's international clients as well as manufacturing operations units and suppliers located abroad. The CFO, Charles Farrow, headed the Finance, Accounting and Investor Relations division and handled all financial and legal matters. The Quality and Improvement division was led by Bruce Isaac and handled KMCO's initiatives for global transformation, process alignment and operational excellence, including the strategic implementation of the enterprise-wide lean and six-sigma process improvement activities, strategy deployment efforts and operational risk management. All division heads, including the CFO, COO and the head of R&D reported to the President Eric Foreman.

Information technology at KMCO

The IT department at KMCO was a part of the quality and improvement division, headed by Bruce Isaac. The IT department under Bruce was primarily responsible for infrastructure management and maintenance. The R&D division, headed by Ralph Danes, was also IT intensive but focused on research and product development. IT staff in R&D were responsible for developing innovative gaming systems and supporting KMCO clients and the company invested heavily in these technology initiatives. The IT staff in Quality and Improvement supported the IT applications and infrastructure needs of the other three divisions (including R&D). In addition to Corporate IT staff, each international and regional location had its own local IT support resources and their own approaches to getting things done.

IT policies and procedures

Owing to the decentralized nature of its IT infrastructure and support staff, KMCO did not employ any formally documented policies and procedures regarding the use of company IT resources. Most of the day-to-day requests like system repairs were handled by email or phone. There were informal documents available for special tasks like setting up new employee systems or departmental moves; however, due to heavy workloads, many employees would simply bypass the procedures.

At the Corporate Headquarters, there were 1300 employees across the major divisions. Approximately 60% of corporate employees conducted some portion of their job duties from home, either as overtime work or due to flexible work schedules. Most employees had personal laptops for conducting company business and were allowed to take their laptops home and connect to the company network over their Virtual Private Network (VPN) connection.

At the different international and regional locations KMCO employees used a variety of IT applications and tools, including in-house developed systems and multiple third-party vendor applications such as instant messaging and email programs. IT support staff implicitly discouraged the use of non-standard vendor software since they found these multiple applications difficult to support. However, due to lack of formal policies regarding software use, employees across KMCO continued to use multiple third-party vendor applications to conduct KMCO business.

Instant messaging

Many of KMCO's business conversations were conducted on Instant Messaging (IM) applications like Yahoo, MSN, etc. Most of the employees used their personal IM accounts to chat with their vendors and also with their relatives, friends and colleagues. At one point, IT estimated that as many as 95% of the company's employees had some sort of IM client installed on their workstations.

From KMCO management's perspective, there was some benefit to allowing employees to use IM. Employees would often check with suppliers to make sure the system development or shipment was complete in order to provide a quick update to the client. Employees also contacted the testing lab for progress checks. IM proved an effective way to communicate when a phone call would be inconvenient but email was too cumbersome. Therefore, KMCO encouraged the use of IM for its ability to facilitate quick business communications. However, because employees used personal accounts and sent both personal and business communications, the IT staff did not provide any support for monitoring or storing IM communications.

Fileserver exchange

Employees across KMCO's divisions were instructed to store documents on shared file servers and to send email attachments through a fileserver exchange. The purpose of this setup was to effectively maintain mailbox sizes and to enable fast exchange of emails. However, the company was facing issues with this mode of transfer. Although a group of users were allocated a folder for file sharing, some employees did not know how to access their shared folder. Even if these employees had access, some users were not sure how to attach files to email. Further, email recipients did not necessarily have access to the same drive as the sender of the email and these access levels were not publicly shared.

Clearly, KMCO employees needed to be trained on how to more effectively use the file server and manage company information. Bruce considered developing policies and procedures regarding acceptable use of IT systems in response to the constant complaints from IT support. The other division heads preferred to keep their IT decisions autonomous and disagreed with this approach. However, in 2003, with the impending Sarbanes-Oxley compliance deadline looming, Bruce was forced to deal with the lack of formal procedures and IT policies soon.

IT compliance and legal issues

Sarbanes-Oxley (SOX) Act – 404 compliance

The Sarbanes Oxley (SOX) compliance project was the first IT compliance-related project undertaken by KMCO. The Sarbanes-Oxley Act introduced in July 2002 brought forth major changes to the regulation of corporate governance and financial practice. KMCO's primary concern with SOX fell under Section 404 of the legislation. That section required firms to publish information in their annual reports concerning the scope and adequacy of the internal control structure and procedures for financial reporting as well as assess the effectiveness of such internal controls and procedures. The Act also mandated that firms retain electronic documents and be able to produce electronic documents when required to do so by the SEC.

Most large, publicly traded companies like KMCO were required to demonstrate initial SOX 404 compliance by mid-July 2005. In anticipation of this deadline, KMCO launched the SOX compliance project in early 2004. KMCO senior management formed an informal steering committee composed of a group of interested members from IT and Legal to manage the compliance initiative. This group did not have a formal charter or mandate regarding the implementation. Nor did they have a vision regarding their purpose. The goal of this project was to evaluate what KMCO needed to do in order to demonstrate compliance, identify software and hardware options for electronic document storage and retrieval and determine the best way to implement the chosen solution.

Implementing the SOX compliance project proved difficult for KMCO. The legal requirements for SOX compliance were complex and IT was not prepared for the additional work load. Additionally, there was continual confusion regarding whether the project responsibility should lie with IT or Legal. As a result, the two groups had communication issues that significantly impeded progress on the project. According to Bruce Isaac, ‘Legal had already conducted some internal changes in financial reporting and instituted changes in our financial audit process. In terms of IT support for these initiatives, we provided whatever support they needed. So it was not a collaborative venture, we simply did what they [Legal] needed.’

The Legal team resented IT’s approach to the project but Charles Farrow championed the initiative. Providing a different perspective on IT’s engagement in the SOX initiative, Charles Farrow said ‘IT’s approach to SOX was that it was a complete waste of time. No one was sure at the time how SOX compliance was truly going to impact us. We had our share of skeptics among Finance and Legal staff. But I tried to remind everyone that the cost of non-compliance could be staggering. But I have to say the IT attitude did not change. Finally, I put my foot down and told my team to take the lead and just send the technical work to IT.’

Despite the challenges, the SOX compliance project team was able to implement some initial controls in compliance with SOX, including implementing an email storage system called Cabinet. The changes were sufficient for KMCO to pass an external audit and avoid penalty. Unfortunately, the SOX compliance project created a rift between Legal and IT. Farrow went as far as stating publicly that ‘for the degree of responsiveness we get with our internal IT, we could seriously consider outsourcing the entire thing. At the least, we will save money and get better service.’ Before these remarks could be taken seriously, Hurricane Katrina hit the gulf coast and KMCO had more serious issues to deal with.

Hurricane Katrina, lawsuit and E-Discovery

Hurricane Katrina hit the US gulf coast in August 2005. Louisiana, the state most severely impacted by Katrina, was a major source of revenue for KMCO, such that the Louisiana revenues were 40% higher than the firm’s average revenues from all other locations combined. Hence, the impact of business interruption and property destruction caused by Hurricane Katrina was high. KMCO had both property and business interruption insurance. However, filing insurance claims required hundreds of hours of IT labor and Legal labor within KMCO (Appendix D). They also employed external legal labor to review all documents that were found. In total, KMCO collected nearly 600,000 pages of relevant and discoverable material. However, they did not give much consideration to the manner in which those documents were located, nor could they guarantee that they had not missed anything.

Just as KMCO was grappling with the insurance claim filing, KMCO’s rival firm, BJH, unveiled its new LCD-based slot gaming systems, integrated with a server-based system providing real-time updates to casino management on player profiles and preferences. BJH’s new system raised alarms among KMCO’s R&D team, because the BJH system was suspiciously similar to a new game concept that KMCO had been developing for the past two years. Ralph Danes had just recently given the team clearance to prepare the upcoming LCD server-based game system for production and authorized the Sales team to begin taking orders. Danes doubted that the similarity between BJH’s new system and his upcoming system was a coincidence. Ralph was convinced that someone within KMCO had leaked the new game concept to BJH and he contacted the other division heads to initiate an internal investigation.

KMCO quickly traced the leak to two of its global sales managers who had recently quit and joined BJH. KMCO was able to locate and produce as evidence certain prototype documents on the KMCO issued laptops of the former employees and some emails sent by the former employees which discussed the product ideas. The division heads were certain that they had a case of corporate espionage against the two former employees, since the employees had the opportunity and the motive to reveal KMCO’s product plans to the rival firm. KMCO filed a lawsuit against its former employees and BJH. However, once the lawsuit was filed, KMCO struggled to produce enough additional evidence that would stand up to legal scrutiny.

KMCO realized that it was time to adopt an efficient IT system to track its internal business records, search these records, and retrieve requested information, without bringing the entire business to a standstill. KMCO had experienced three major events in succession, each of which pointed to the weaknesses of their infrastructure and processes for storing and retrieving electronic information. The SOX project, Hurricane Katrina insurance claim, and BJH lawsuit were major undertakings that required extensive manual labor from IT and Legal staff combined. KMCO also dealt with smaller legal and insurance issues several times a year and the division heads decided that it was time to find a better way to handle such matters. KMCO decided to undertake an E-Discovery project to address this concern.

Electronic discovery (E-Discovery) refers to any process in which electronically stored information (ESI) is stored, located, secured, and searched so it can be used as evidence in a legal case. Such information should be collected and preserved in a manner that enables it to be systematically searched, accessed and retrieved, if and when required for legal proceedings. In addition to Sarbanes Oxley concerns, the importance of strategically managing electronically stored information was highlighted with the enactment of federal regulations such as Health Insurance Portability & Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLB). Further, guidelines issued by agencies such as Securities and Exchange Commission (SEC), National Association of Securities Dealers (NASD), and NYSE contained strict rules regarding the preservation and destruction of a firm's business records.

Additionally, in December 2006 the Federal Rules of Civil Procedures (FRCP) were amended to include guidelines for discovery of electronic documents as evidence in civil lawsuits. FRCP does not mandate compliance like federal regulations such as SOX or HIPAA, but when faced with a civil lawsuit, firms are expected to be able to provide an inventory of their electronic data sources in addition to providing appropriate electronic information within timeframes and in appropriate formats, as mandated by the courts. These guidelines meant that communications such as emails, internal memos, and instant messages could be used as evidence of a firm's conduct and policies and hence such material would be target of discovery. The guidelines covered both computer-stored records (active data, replicated data, residual data, backup data, and legacy data) and computer-generated records (cache files, cookies, Web logs, and embedded data or metadata). Firms were also required to show a legally credible, computer use and operation policy that would lend credence to the e-records furnished by the firm.

Although KMCO filed its lawsuit against BJH prior to the FRCP amendment, KMCO was subject to the amended guidelines. The combined effect of the filing of lawsuit and the FRCP amendments further magnified KMCO's need to select an E-Discovery tool.

The E-Discovery project

After consideration of the issues, KMCO's Board commissioned an informal steering committee with representation from all divisions to provide recommendations on such a project. The committee decided to take stock of the existing application and infrastructure landscape to determine how to streamline the management of e-records. Some of the inefficiencies discovered in KMCO's existing infrastructure were:

- There was no uniform archiving policy at KMCO and no organized way to automate document search and retrieval. When older emails were required, it took weeks of searching across multiple storage media to find them.
- The email retention policy was also not standard. Some users could permanently delete their emails and attachments, which led to loss of important data.
- The version control software was not integrated with archiving. Finding the final version of contracts or important documents such as insurance policies also required searching and comparing multiple versions before determining the final version.
- A variety of financial analyses were computed on spreadsheets. These spreadsheets, often sent as email attachments, had multiple versions and the final version was not documented or archived. KMCO was often unable to determine whether the final version of important spreadsheets was available or had been shredded.

By April 2006, the committee had identified the relevant sources of ESI at KMCO. ESI consisted of emails, email attachments, text and word processing documents, spreadsheets, acrobat reader documents, corporate and intranet web pages, voice mail on KMCO's corporate phone lines and KMCO issued cell phones and personal digital devices (used by KMCO employees) and fax documents. The committee also identified the locations where this ESI was stored, including internal computer networks, enterprise resource planning (ERP) databases, communications servers (with fax, voice mail and emails), backup tapes and servers and finally the electronic devices assigned to individuals (e.g., desktops, laptops, Blackberry™ phones). The committee prepared a lengthy report detailing the results of their work.

However, when Bruce read the report, he was concerned. Bruce personally knew of additional servers that were not listed in the report because they were stored in international or satellite locations. For this reason, Bruce wanted IT to conduct a full company-wide audit to uncover all ESI that would fall under the US legislations, regardless of whether it was stored in an off-site location. In addition to this audit, Bruce wanted to develop a comprehensive E-Discovery project plan including controls for restricting system access and tracking all company communications through its various communication mediums.

This suggestion however was vetoed by all the KMCO division heads. Legal staff were already struggling to manage the document requests from the insurance firm for the Hurricane Katrina claim. Manufacturing and global supply were also actively dealing with the Katrina aftermath, focusing on increasing production to make up for lost sales in the gulf coast. Even R&D was opposed to the idea; Bruce's mention of 'controls on access and use' was instantly perceived as a barrier to the creative product development work and encroachment on R&D's territory. Given the opposition, Bruce decided the committee should eschew the audit and move on to the next step.

E-Discovery – recommended approach plan

The committee prepared a plan for achieving the E-Discovery project objectives and submitted it to the board for review. The plan was a three-pronged approach covering organizational policies, infrastructure and tools. The committee recommended implementation in four stages:

1. *Phase One: Creating an IT use policy framework* – Defining and communicating organization-wide policies regulating the access and use of KMCO infrastructure and computer equipment, including:
   a. Internet use by KMCO employees
   b. Network and IT equipment
   c. Remote access policy
   d. Rules for storage, retrieval, and destruction of ESI
   e. Procedures to follow when responding to E-Discovery requests
2. *Phase Two: Assessing and preparing for infrastructure upgrade* – The guidelines and policies articulated in

phase one would require substantial investments in infrastructure to support ESI storage and retrieval. The technical requirements would include:

a. Substantial investment in media storage equipment for archiving data and enhancements to back-up technology.
b. Implementing or upgrading existing VPN infrastructure and security rules

3. *Phase Three: Selecting a records management tool* – The IT use policies and infrastructure upgrade would pave the way for installing tools to help manage e-records and assist in searching and retrieving records (see Appendix E for more information on tools and delivery models).
   a. E-Discovery Tools: A wide range of tools to support E-Discovery, email archiving, information access and content management are available. KMCO would need to determine whether to acquire an all-in-one solution to store all types of ESI, or implement multiple tools to store specific types of information. There were pros and cons for each option.
   b. Delivery Model: Once the E-Discovery tools are selected, KMCO would have to decide whether to internally implement the process of upgrading their infrastructure to support the new tools (including migrating all ESI) or hire a vendor to manage the implementation.
4. *Phase Four: Maintenance and audits* – The E-Discovery process may need to adapt itself to changes in federal laws and guidelines. Additionally, with changes in technology, IT equipment and usage, the vulnerabilities in the system may need to be continually identified and corrected. Internal audits that routinely subject the system to thorough analysis were recommended. This would also ensure that the policies framed at the organization level were being followed appropriately.

The board commended the committee for its thorough study and wide-ranging recommendations. However, with the urgent need to start effective E-Discovery, the board issued two decisions:

1. The IT division should proceed with helping Legal and Finance staff deliver its E-Discovery tool in support of the Hurricane Katrina insurance claim (partially implementing phase three of the plan only). Once that effort was complete, similar tools were to be implemented across KMCO.
2. The committee should be disbanded since its task of making recommendations was now complete. The Board would be willing to reconsider the need for organizational policies and more substantial infrastructure upgrades (the remaining phases of the plan) later. IT would be responsible for completing the remaining work later.

E-Discovery implementation

Owing to the board's decision, the IT division was forced to try to select and deliver an appropriate E-Discovery tool without having a best practices framework to follow and potentially without the infrastructure to fully support the implementation. Bruce decided that IT would start with the tool selection as decided by the board, then would move forward with the policy and infrastructure upgrades as well. A project team comprising managers and team leads from IT was formed.

The project team drafted an implementation plan to identify the most critical areas in need of immediate improvement. They realized that a key area for E-Discovery was archiving. They currently had a routine backup plan and a disaster recovery plan but archiving needs were different and neither backup data nor disaster recovery systems could be used to provide the records needed by a legal discovery process. While backup and archiving were both methods of copying the stored data, backups often allow overwrites to backed up data and could be used in parallel with live data. Archiving implies that the data archived is now deleted from the live data used for business transaction and the archived data is the only copy of the data available.

Archiving provides superior performance and allows firms to retain historic data for data mining and business intelligence purposes. Archiving is also a key aspect of compliance. However, archival storage is expensive and given the rate at which records are generated, storage requirements can increase exponentially since records cannot be deleted without taking into account the federal and state rules that mandate records retention. Searching, accessing and producing records from the archive are complicated as well. Hence an ideal policy would have to achieve a trade-off between storage costs, legal requirements and search capability.

Archiving KMCO's ERP systems and databases was not foreseen as troublesome. However, the email environment was complex. The MS Outlook server had anti-virus, anti-phishing, anti-spam software filtering emails. This immediately added a layer of complexity to archiving all emails. Every email could have multiple respondents and multiple variations. The archiving policy had to take an integrated approach by assessing the reporting environments and logs of each of these tools in the email environment. In addition to these complexities, the Finance division had already implemented Cabinet Systems as a part of the SOX compliance project. The project team needed to determine whether to deliver Cabinet to other departments, support multiple email archiving tools at KMCO, or implement a new enterprise tool and require that Legal and Finance discontinue use of Cabinet.

Bruce considered the pros and cons of implementing Cabinet across KMCO. Since the legal/finance division was already working against a tight deadline attempting to deliver the documents required for filing insurance claims, Bruce did not think disrupting their email environment with a new archiving tool would be healthy. KMCO already had licenses for Cabinet and hands-on experience with the tool. Therefore, they ultimately implemented Cabinet company-wide. However, Cabinet did not support any other document management needs except emails. That meant IT would still need to implement and support multiple tools in the future.

Outcomes

E-Discovery project

Soon after the implementation, KMCO realized the disadvantages of implementing Cabinet as an enterprise solution. Cabinet was not able to support KMCO's implementation with patches and updates as efficiently as Bruce's division had expected. Cabinet had recently added file archival, data protection and recovery and E-Discovery tools to its suite, however, Cabinet's capabilities as an E-Discovery suite had received very unfavorable ratings in recent product reviews. Cabinet also had limited functionality and support for global implementation outside North America. The IT division was reluctant to continue to use Cabinet for all its E-Discovery needs.

Lawsuit against BJH

In April 2008, KMCO lost its lawsuit against BJH. KMCO had submitted evidence including emails from the employees discussing the product ideas and prototype documents found on the former employees' laptops. However, the former employees were able to question the reliability and the credibility of KMCO's evidence. They pointed out that the laptops were guarded by weak passwords, which were often shared and rarely changed. Hence the documents were found on the laptop but not ascertained to be saved/stored there by the former employees. Additionally, while the copies of emails were provided as evidence, KMCO's search processes had not taken into account persons marked as BCC (blind carbon copy) – individuals who were also previously employed at KMCO and had comparable opportunity and motive to sell/distribute KMCO product ideas to competition. Neither was KMCO able to show a standard archiving policy which could verify that the emails produced into evidence had not been manipulated later.

KMCO did know that employees frequently used third-party IM chats, but since these were not archived, KMCO could not produce any chat conversations of the former employees as evidence. KMCO, despite being able to search and locate some relevant electronic information, was not able to establish that its computer operating procedure was standard, justifiable and that its electronic data was forensically protected. These omissions were enough to weaken KMCO's case against BJH.

Next steps

The question KMCO had to address at this juncture was how or whether to proceed with the ERM and E-Discovery project. Bruce knew that everyone was looking at him now for guidance, but what steps should he take next?

Questions to consider:

1. What is E-Discovery? Why did KMCO need/want to implement E-Discovery?
2. What was KMCO's approach to implementing E-Discovery? What current (or potential) weaknesses do you see in this approach? How prepared is KMCO to deal with another lawsuit?
3. How well does the E-Discovery Reference Model provide the ability for KMCO to maintain compliance with Sarbanes-Oxley or other US and international legislation? Can you think of other frameworks (beyond the E-Discovery Reference Model) that might also work for KMCO?

About the authors

Christina N. Outlay (coutlay@depaul.edu) researches and teaches at the School of Accountancy and MIS, College of Commerce at DePaul University. Her research interests focus on human resource issues in IT outsourcing, legal issues in IT, accounting information systems and health-care IT. Before entering academia, she spent several years in industry in IT project and program management. Her research has appeared in venues such as *MIS Quarterly Executive*, *Proceedings of the International Conference on Information Systems* and *Proceedings of the Academy of Management Annual Meetings*. She received her PhD in Management Information Systems from the University of Illinois at Chicago, and master's degree in Information Systems from DePaul University. She also holds Project Management Professional (PMP) and ITIL Foundations professional certifications.

Poornima Krishnan (purikrishnan@gmail.com) currently teaches as part-time faculty at North Central College. Her research interests include outsourcing governance, offshore outsourcing management, IT compliance and quantitative research methods. She has published and presented her work in conferences such as International Conference on Information Systems and Academy of Management Annual Meetings. She has also worked in industry in different business/IT roles before entering the doctoral program. She received her PhD in Management Information Systems from the University of Illinois at Chicago and an MBA degree from Narsee Monjee Institute of Management Studies, India.

Chandrasekaran Ranganathan (ranga@uic.edu) researches and teaches at the Department of Information and Decision Sciences, University of Illinois at Chicago. His current interests include IT outsourcing, strategic management of information systems, health-care IT and business value of IT investments. His research has appeared in several journals and conference proceedings. He is the winner of the Best Doctoral Dissertation Award and the Best Teaching Case Award at the International Conference on Information Systems, and he is also a three-time award winner of SIM's Paper Awards Competition. He holds a doctorate from the Indian Institute of Management, Ahmedabad, and a master's degree from BITS, Pilani, India.

Appendix A

See Figure A1.

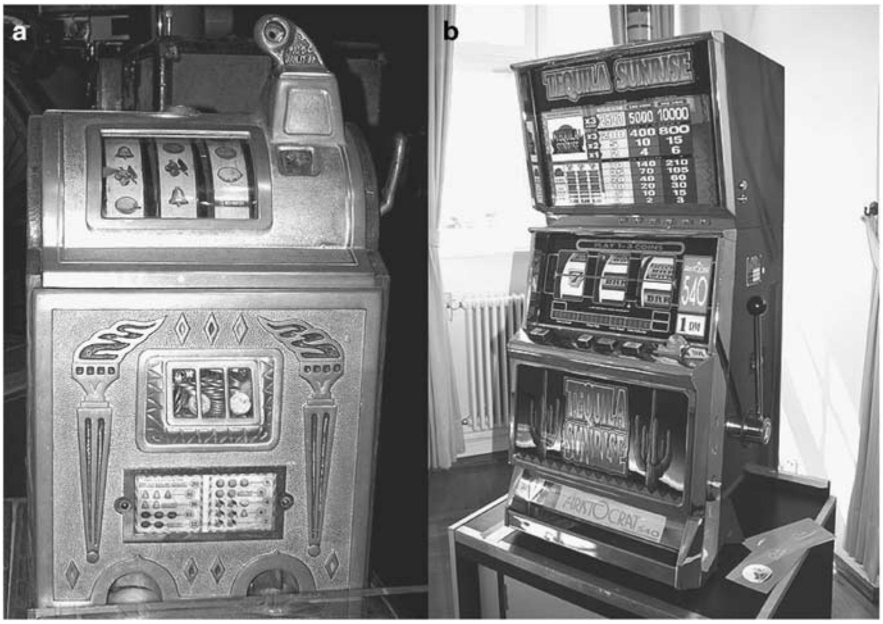

Figure A1 Example traditional mechanical game systems.
a) Source: http://commons.wikimedia.org/wiki/File:Old_slot_machine.jpg.
By Valerie Everett from Indianapolis, USA (Old slot machine) [CC-BY-SA-2.0 (www.creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons.
b) Source: http://commons.wikimedia.org/wiki/File:Slot_Machine_Tequila_Sunrise.JPG.
By Stefan-Xp (Own work) [GFDL (<a href = 'http://www.gnu.org/copyleft/fdl.html' class = 'external free' rel = 'nofollow' > http://www.gnu.org/copyleft/fdl.html < /a >) or CC-BY-SA-3.0 (www.creativecommons.org/licenses/by-sa/3.0/)], via Wikimedia Commons.

Appendix B

See Figure B1.

Figure B1 Example server-based game system.
Source: http://commons.wikimedia.org/wiki/File:Norwegian_Slot_Machine.jpg.
By Sjurmh (Own work) [CC-BY-SA-3.0 (www.creativecommons.org/licenses/by-sa/3.0) or GFDL (< a href = 'http://www.gnu.org/copyleft/fdl.html' class = ' external free' rel = 'nofollow' > http://www.gnu.org/copyleft/fdl.html < /a >)], via Wikimedia Commons.

Appendix C

Hurricane Katrina insurance losses

KMCO's Louisiana facility was covered under both property damage and business interruption insurance. In order to file property damage insurance claims in the aftermath of Hurricane Katrina, KMCO needed to produce a record of the assets they owned, and provide a verifiable estimate of the value of the assets. Then, based on the estimate of the damage caused to the assets by the hurricane, the insurance firm would determine the amount to be paid for the claims. Similarly to file business interruption claims, KMCO had to quantify the length of time for which the business was interrupted and the consequent losses incurred, in order to receive compensation from the insurance company.

Property damage losses

For KMCO, the property damage claim filing process was complicated since they had minimal record of what was in their offices and buildings that were damaged by the hurricane. Additionally, KMCO equipment at several casinos was damaged but the records for leased equipment were managed at the local KMCO offices. Since they did not have immediate access to this information, they had to spend months piecing together this data from files stored on central servers and employee systems. This process cost them valuable time and money, and it also delayed the rehabilitation of their facilities and work in Louisiana.

Business interruption losses

To file their business interruption claim, KMCO had to track revenues and expenses for Louisiana facilities from company documents. They also had to establish the typical revenues from the Louisiana operations when it was interrupted by the hurricane, so they could claim appropriate insurance compensation.

A robust records and asset management system can help firms like KMCO track every asset across office locations and allow them to get a clear picture of the location of the assets, as well as the potential replacement costs of the assets if there is a natural disaster in that location. Typically, implementing such asset management systems also reduces insurance premiums for firms.

Appendix D

E-Discovery tools and expenses

There are multiple tools available to serve firms' E-Discovery needs. Some tools provide niche functionality (e.g. GWAVA, Metalogix). Product suites are also available that cover the gamut of E-Discovery needs (e.g. Mimosa systems, Symantec, EMC).

In addition to matching internal needs, volume of data to the features provided by these tools and product suites, firms also need to consider the cost of E-Discovery process and select a delivery management that best suits their needs. One option is to install E-Discovery tools and train internal staff to handle the E-Discovery process. This option requires firms to train internal IT and legal staff in managing these requests and firms also have to budget for maintaining and upgrading their E-Discovery products. The second option is to outsource the delivery of E-Discovery process to external vendors, letting them assume responsibility to update and manage the E-Discovery products. With the exception of routine audits and monitoring, this option requires minimal internal training for handling E-Discovery. However this maybe a more expensive option for firms, especially if their volume of E-Discovery requests is small.

Sample of expenses involved in responding to E-Discovery requests:

- Data Collection: Expenses may vary depending on whether the data is archived or in active use.
  - $250–500 per hard drive or backup tape
  - $2000–3000 per server

- Locate, search and retrieve data using indexing and search tools
  - $1800 per hard drive (extracting data from backup tapes is more expensive)
  - $450 per email inbox

- Collate Relevant Data
  - $750 per hard drive to prepare data for production in proper format

- Transform data into acceptable format for legal proceeding
  - $4 per MB plus $0.10/page for Bates numbering and tiffing (converting images into '.tif' format) the images

Document retention	*Email archiving*	*Data and records management*	*Indexing and search*
Retention and management of documents and content created across the organization, for example, pdf files, word documents, PowerPoint files, etc.	Capture, store and manage all email communications within the organization. This includes capturing communications on calendar, smart phones and deleted emails.	To capture, store and create back-ups for all applications, application data, and version changes.	Ability to index, locate, search and retrieve electronically stored information (ESI). Includes emails, attachments, files, IM and other content generated within the organization.

Appendix E

See Figure E1.

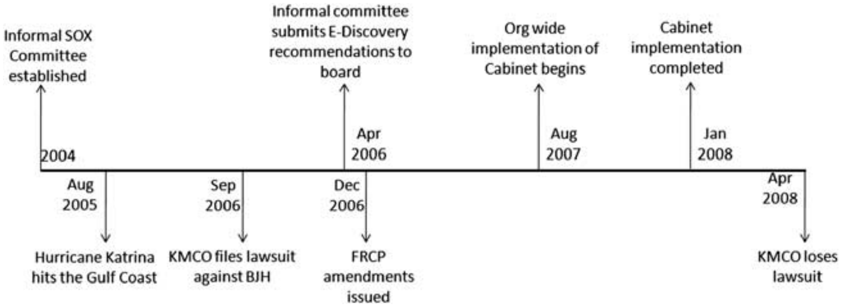
Informal SOX Committee established
2004
Aug 2005
Hurricane Katrina hits the Gulf Coast
Sep 2006
KMCO files lawsuit against BJH
Informal committee submits E-Discovery recommendations to board
Apr 2006
Dec 2006
FRCP amendments issued
Org wide implementation of Cabinet begins
Aug 2007
Cabinet implementation completed
Jan 2008
Apr 2008
KMCO loses lawsuit

Figure E1 KMCO timeline.