Trade Secret Law and Information Systems: Can Your Students Keep a Secret?

Lorrie Willey
Janet C. Ford
Business Administration and Law
Western Carolina University
Cullowhee, NC 28723, USA
lwilley@email.wcu.edu jford@email.wcu.edu

Barbara Jo White
Danial L. Clapper
Computer Information Systems
Western Carolina University
Cullowhee, NC 28723, USA
whiteb@email.wcu.edu clapper@email.wcu.edu

ABSTRACT

The impact of intellectual property (IP) law on information systems (IS) professionals in business cannot be overstated. The IS 2010 model curriculum guidelines for undergraduate IS programs stress the importance of information security and knowledge about IP. While copyright and patents are the most well-known types of IP, another, trade secrets, which involve confidential information generated by business to secure financial success, poses a unique challenge partly because IS professionals are often less familiar with trade secrets as a form of IP. Just as important is the crucial role IS plays in actually creating trade secrets. Information must not only be vital and proprietary but also its secrecy must be actively protected and maintained against data security challenges, including unethical behavior by disgruntled employees, corporate espionage, and inadvertent disclosure. Failure to do so results in a determination that information is not legally a protected trade secret. Unlike copyrights and patents, information cannot publically be designated as a trade secret prior to a challenge. Instead, organizations must prove the information is actually a trade secret. Critical to this proof are processes and internal systems businesses use to maintain information secrecy, which determine whether legal remedies exist if the trade secret is wrongfully divulged. This paper discusses trade secret law, methods used to secure trade secrets, and the role of IS in supporting and/or developing those methods. A class exercise provides IS students with insights into trade secret law and acceptable, ethical conduct of IS professionals who protect trade secrets.

Keywords: Intellectual property, Information assurance and security, Instructional pedagogy, Team-oriented problem solving, Active learning

1. INTRODUCTION

In 2010, the IS community released a major update to its undergraduate curriculum guidelines that encompasses not only technical knowledge and skills but also managerial knowledge and skills (Topi et al, 2010). The 2010 guidelines identified seven key capabilities that high-performing IS graduates should demonstrate upon completion of their IS degree: "improving organizational processes; exploiting opportunities created by technology innovations; understanding and addressing information requirements; designing and managing enterprise architecture; identifying and evaluating solution and sourcing alternatives; securing data and infrastructure; and understanding, managing and controlling [information technology] IT risks" (Topi, et al., 2010, pp.362).

These capabilities reflect "the change in the nature of the jobs IS graduates are likely to have by focusing on business analysis, organizational processes, enterprise architecture, sourcing options, and security/risk management" (Topi, et al., 2010, pp. 375). In addition to these capabilities, the guidelines expect that IS professionals will "exhibit strong ethical principles and have good interpersonal communication and team skills" (Topi, et al., 2010, pp. 370).

To this end, the guidelines encourage educational experiences that require students to identify and evaluate ethical issues in the IS field, work with others in the IS field and outside of the field, and demonstrate effective communication (Topi, et al., 2010).

The guidelines recognize the need for IS students to be familiar with the legal environment in which they will work and identify several courses that would be appropriate delivery points for this information and experience. For example, in IS project management courses, students need to "understand the mechanisms for dealing with legal issues" (Topi et al, 2010, pp. 398), while in IS Systems Analysis and Design, students need to "analyze and articulate ethical, cultural, and legal issues and their feasibilities among alternative solutions" (Topi et al, 2010, pp. 400). In IT Security and Risk Management courses, students need to learn to secure information assets and mitigate effects of legal prosecution. Further, the guidelines suggest that specific knowledge areas of IS include professional IS issues such as ethical and legal issues, intellectual property, and privacy (Topi et al., 2010). This paper focuses on aspects of intellectual property, specifically trade secrets, and data security that need to be addressed in the IS curriculum.

2. WHY IP LAW IS IMPORTANT TO IS STUDENTS AND PROFESSIONALS

Creativity has long been considered a foundation of the American economy and has been protected by law since this country's inception through the grant of constitutional protection (U.S. Constitution, art. I, § 8). Accordingly, under United States IP laws, the purpose of IP protection is two-fold: to provide a financial boon to the inventor or creator of the work and to promote creativity, which drives economic growth by keeping information in the public domain (Lao, 1998). The two IP forms that most IP professionals and students are familiar with are copyright and patent. Generally speaking, copyright law grants certain exclusive rights to those who produce original creative works while patent law grants certain exclusive rights to those who produce new inventions or processes. Copyrights and patents are often used to protect business process and software development and as such, IS professionals encounter those forms of IP and the legal protections they are afforded (Ford, et al., 2010). However, another important form of IP is trade secrets, which are generally defined in the U.S. as proprietary information that generates an economic advantage for a particular business (UTSA 1985, section 14).

When it enacted the Economic Espionage Act, Congress recognized "the great importance of trade secrets to the national economy, going so far as to equate threats to trade secrets with threats to the country's national security" (Brenton, 2009, pp. 454.) In the information age, IP protection is hailed as one of the great driving forces of the economy (Administration, 2008). In fact, "reliance on modern technology has resulted in intellectual property comprising a substantial portion of the business assets of modern commercial enterprises" (Beckerman-Rodau, 2002, pp. 228). IP currently constitutes approximately 70 percent of U.S. business assets (Pacini et al, 2009). The U.S. Department of Commerce values America's intellectual property at over $5 trillion (Administration, 2008). With IP playing an essential role in the economy, professionals and students in IS-related disciplines must be aware of the role their discipline plays in supporting the continued growth and protection of IP, including copyright, patent, and the lesser-known area of trade secrets.

IS-specific activities are crucial not only to the protection, but also the creation of trade secrets and other proprietary information providing competitive advantages. In securing protection for trade secrets, IS professionals play a unique role in creating the systems and processes necessary to maintain the secret information. Increased use of technology has made the protection of trade secrets more difficult while simultaneously providing tools to protect trade secrets. In fact, legal protection is afforded largely on the efforts businesses make to keep identified information secret. To this end, businesses and trade secret owners depend on their IS professionals to secure this top-secret information. Recognizing the increased need for IS students to understand their role in securing intellectual property, course specifications in the IS 2010 guidelines outline learning objectives, topics, and suggested activities that help meet this need. The table on the following page represents courses in which a discussion and study of trade secret law would be appropriate according to the IS 2010 Guidelines.

3. TRADE SECRET ESSENTIALS FOR IS STUDENTS

Successful implementation of the IS 2010 guidelines regarding security and IP require a basic understanding of trade secret law, which is an area of intellectual property law distinct from copyright law and patent law. Significantly, copyright and patent law requires that specific criteria be met to qualify for protection and also requires that the information be made public. Trade secrets, however, need not meet these criteria and their value lies in not being made public. While copyrights and patents are both protected by federal law, the most common source of trade secret protection, and one which provides some consistency between states in this area is the Uniform Trade Secret Act (UTSA). Forty-five states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have adopted the UTSA. Of the states that have not adopted the UTSA, two, Massachusetts and New Jersey, introduced legislation in 2011 to adopt the UTSA (Legislative Fact Sheet, n.d.). North Carolina has adopted a Trade Secret Protection Act that contains provisions similar to the UTSA (North Carolina Trade Secret Protection Act). New York and Texas continue to apply common law principles rather than follow a statutory scheme (*Ashland Management*, 1993 and *In re Union Pacific R. Co.*, 2009).

The UTSA broadly defines a trade secret as:

> …information, including a formula, pattern, compilation, program, device, method, technique, or process, that:(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
>
> (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. (UTSA 1985, §1(4)).

The value, or potential value, of a trade secret lies in the economic advantage provided by the secrecy of the information. Should the information become publicly known, legal protection, as well as any economic advantage, is lost. Trade secrets may be compromised through deliberate misappropriation (theft) of secret information, or through its

Course Title	Learning Objectives	Topics	Notes
IS 2010.1 Foundations of Information Systems (Core Course)	• Mitigate risks as well as plan as well as plan for and recover from disasters	• Information systems ethics and crime (p 393)	
IS 2010.4 IT Infrastructure (Core Course)	• Understand the differences and similarities between the core elements of an IT infrastructure solution, such as clients, servers, network devices, wired and wireless network links, systems software, and specialized security devices • Analyze and understand the security and business continuity implications of IT infrastructure design solutions • Configure simple infrastructure security solutions	• Securing an operating system • Securing IT infrastructure (Principles of encryption and authentication; component level security: clients, servers, storage network devices, data transport, applications; Perimeter security: firewalls; Using public networks for secure data transport: VPNs	• Whenever possible, it is recommended that this course [use] hands-on laboratory work and practical exercises to teach the complex concepts that are often too abstract to grasp without practical examples.
IS 2010.6 Systems Analysis and Design (Core Course)	• Articulate various systems acquisition alternatives, including the use of packaged systems • Compare the acquisition alternatives systematically • Analyze and articulate ethical, cultural, and legal issues and their feasibilities among alternative solutions	• Analysis of project feasibility (legal) • Analysis and specification of system requirements (factors affecting security)	• Using a course project is highly recommended • The course specifically emphasizes the importance of incorporating security issues … from the earliest stages of the course
IS 2010.7 IS Strategy, Management, and Acquisition (Core Course)	• Understand how strategic decisions are made concerning acquiring IS resources and capabilities including the ability to evaluate the different sourcing options	• IS risk management (managing security and privacy)	• Using a case study methodology is highly recommended for this course as it will help the students strategically identify issues in a real-world setting
IS 2010 IT Audit and Controls	• Identify risks to the [confidentiality], integrity, and availability • Understand best practices, standards, and regulatory requirements governing information and controls that may vary for an organization's locations and customers. Gain the ability to measure the degree of compliance with them	• Encryption, authentication and non-repudiation	• The use of case studies, professional standards, and sample audit software programs are encouraged to exemplify concepts covered
IS 2010 IT Security and Risk Management (Elective Course)	• Design and guide the development of an organization's security policy • Determine appropriate strategies to assure confidentiality, integrity, and availability of information • Apply risk management techniques to manage risk, reduce vulnerabilities, threats, and apply appropriate safeguards/controls	• Inspection, Protection, Detection, Reaction and Reflection • Risk assessment frameworks • Security engineering • Physical aspects • Security in connected systems and networks • Policy and management issues (copyright and privacy protection)	• The use of case examples for discussion and reflection in this course is highly recommended • It is recommended to include an applied project for a potential client in which students conduct a risk assessment of a part of the client's IT infrastructure

Table 1: IS 2010 course specifications that relate to trade secret course activity (Topi et al, 2010)

disclosure, whether deliberate or inadvertent, and the UTSA applies to both. Remedies under law reflect damages for the disclosure of information, the loss of the economic value of the information, and injunctive relief to prohibit the continued disclosure of information maintained as a trade secret (UTSA 1985, §§ 2-3).

Once the information a business desires to protect has been identified, the next step is to secure the secrecy of the information. In this area, courts look closely at specific measures businesses take to maintain the confidential nature of the information. There should be a balance between the value of the information to be maintained secretly and the costs associated with the measures taken to secure the information. (Rockwell Graphic Systems, 1991). Should trade secret litigation arise, courts look at the reasonableness of the measures taken to maintain secrecy under the circumstances particular to that dispute. Reasonable measures include physical controls, such as doors, locks and signs, and technological controls such as restrictive access to information stored digitally (Pacini et al, 2009). "Data security is critical to trade secret protection because the value of a trade secret lies entirely in its secrecy" (Rowe, 2010, pp. 749).

Traditional methods of preserving secret information are still utilized by trade secret owners. Employees are given access to confidential information only on a need-to-know basis and those who do have access sign non-disclosure and non-compete agreements with their employers (Pacini et al, 2009). Moreover, employee training on the nature of trade secrets and exit interviews for departing employees are routine practices for a business making reasonable efforts to maintain trade secret protection (Pacini, et al., 2009).

Trade secret documents include clear legends noting the confidentiality of the information, and the fact that the information is a trade secret. The retention and copying of those documents is generally controlled (*Tedder Boat Ramp Systems, Inc*., 1999). These controls reflect fundamental processes regarding access to and the dissemination of trade secret information.

Traditional means of securing data, though, are not sufficient when trade secret information is stored in digital form, and this creates a responsibility for IS professionals to secure data from threats associated with technology. "There is a tension between the need to keep information secret and modern technological methods that allow the information to be easily accessed, reproduced, and disseminated" (Rowe, 2009, pp. 15). "The digital world is no friend to trade secrets" (Cundiff, 2009, pp. 362).

IS professionals take a leading role in protecting the secrecy of digital trade secrets by establishing security systems and auditing those systems regularly to ensure that the valuable data remains secure and that the systems continue to serve that purpose. It makes sense then, that IS students be exposed to a curriculum that explores these demands and gives them opportunities to develop their skills in the data security and IP area.

4. THREATS TO DIGITAL TRADE SECRETS

The tools that serve to make business more efficient and productive are the same tools that make the protection of trade secrets more problematic for the trade secret owner (Rowe, 2009). Trade secrets are increasingly stored in digital form (Brenton, 2009), which makes them both easier to store and easier to share. The vulnerability of trade secrets is illustrated by a recent estimate that the theft of IP costs business approximately $59 billion annually (Pacini et al, 2009).

In this digital environment, the reasonable efforts required by law to maintain the security of trade secrets and legal protection of those secrets rests squarely on the shoulders of IS professionals. It is a special challenge that in the area of trade secrets, there is a need for both technical and legal knowledge (Green, 2007). Securing information includes identifying sensitive information, restricting and monitoring those who have access to the information and monitoring where the data goes (Wiens, 2007). That requires trade secret holders to coordinate closely with IS personnel to keep abreast of advances in technology that give rise to new threats, or that provide improved protection of the confidential information (Cundiff, 2009). The next sections will examine some of the key threats to trade secrets owners in a digital world.

4.1 Portable devices: Loss or theft of data

Given the ubiquitous presence of desktop computers and the proliferation of laptops, smartphones, USB drives, Mp3 players and other mobile electronic devices, stored information is readily portable. This is particularly alarming to business since 90 percent of stolen laptops are never recovered, and 57 percent of corporate crimes are linked to laptops (Yip, 2006). IS must assist the trade secret owner with developing policies for travelling with laptops, the use of privacy screens, using a clean hard drive rather than one filled with data when travelling, the storage of data on USB drives and maintaining possession thereof (Cundiff, 2009). Since laptops are easily lost or stolen, employees need to be educated regarding the risks associated with laptops and be trained on the proper procedures if they are forced to travel with trade secrets on their laptop. The proper use of cable locks, complex passwords, and the deletion of data from the laptop after use are examples of those types of procedures.

4.2 External Threats: Hackers

Hackers use a variety of methods to compromise the integrity of a network and access secure systems and trade secrets (Cundiff, 2009). Storing confidential information that can be accessed by remote networks increases risks that the information can be intercepted by third parties (Beckerman-Rodau, 2002). Implementing robust perimeter controls and security measures, such as intelligent firewalls and intrusion detection software, is crucial, as are other security best practices that IS professionals use to protect their network from attack such as strong encryption and segmenting access to information (Green, 2007).

4.3 Internal Threats: Well-intentioned Employees

The widespread use of electronic communication such as email, networks, blogs, and social media, poses increased risks to the confidentiality of trade secrets (Lau, 1998). In this environment, it is possible for even a well-intentioned employee to inadvertently divulge trade secrets. A posted trade secret can potentially be disclosed to a worldwide audience.

While courts are divided over whether posting trade secret information automatically destroys the protected secret, the risk is high. Courts consider how quickly trade secret owners make efforts to remove posted information. However, even if efforts are made, removing posted data is difficult. While trade secret owners should request that wrongfully-disclosed data be removed from search engines, no law compels such removal (Rowe, 2007). To make things worse, exposure of a trade secret for any amount of time negatively affects its economic value, which is based on its secrecy (Beckerman-Rodau, 2002).

Obviously, a goal for preserving trade secrets is to never have confidential data on the network or at least isolating and security sensitive data from the public networks (Rowe, 2007). For well-intentioned employees, the most valuable tool in prevention is training. All employees with access to trade secrets must clearly understand what those trade secrets are and know precisely what they can and cannot communicate about them in a public setting.

Owners can also prohibit employees from going to storage sites online, disable or eliminate USB ports, provide guidelines for safe access to data offsite, specify how data will be deleted, and utilize periodic certifications that identify all storage devices to which employees have transferred data. Digital watermarks, legends to identify secret document- controlled access to sensitive data and secure intranets can help to ensure that the employee recognizes and consequently protects company trade secrets (Cundiff, 2009).

4.4 Internal Threats: Disgruntled Employees

If well-intentioned employees have the potential for endangering trade secrets, disgruntled employees represent a potentially catastrophic threat. Current or former employees account for 85 percent of trade secret theft (Rowe, 2010). Trade secrets are frequently compromised by employees who leave jobs, often to go work for a competitor, and download sensitive data on such items as parts, components, assembly sequences and customer lists (*Diamond Power International, Inc.*, 2007) or download price lists (*Liebert*, 2005) to USB drives or laptops prior to leaving their jobs.

Trade secret owners should implement physical access control to trade secrets, as well as control of storage media used by employees when working with trade secret data or when they are in facility areas that allow access to trade secret information (Beckerman-Rodau, 2002). In addition, the company should have a clear policy on the termination of computer access by departing employees and have procedures in place to ensure these policies are being followed.

Given the insider status of current employees, they have a much easier task than an external hacker to access company secrets by disabling or circumventing security systems and controls. Systems should be considered that would allow IS to track access to files, when files are copied, when files are transferred and when files are deleted (Cundiff, 2009), although if the disgruntled employees work in IS, it is possible they could avoid detection. Social media such as chat rooms and blogs provide the means for employees to post their employer's trade secrets. These sites can easily be monitored by competitors in the search for postings of trade secret information (Beckerman-Rodau, 2002). Employees have emailed trade secrets to employees working for competitors (*Posdata Co. Ltd*., 2007). In addition to allowing the easy transfer of information, email may be backed up on several servers unknown to the trade secret holder (Beckerman-Rodau, 2002). Resources such as eWatch, CyberCheck, Cyvellience, can be utilized by the owner to monitor the web to determine if protected information is on the Web or on the web sites of competitors, chat rooms, financial, professional social network sites (Cundiff, 2009).

4.5 Corporate Espionage

Corporate espionage is also a threat to the security of trade secrets. Some techniques used to conduct such espionage include "scanning trade show floors, combing through websites …taking photographs of factories and businesses, using data-mining software to search databases on the internet, stealing laptop computers, dumpster diving…" (Pacini et al, 2009, pp. 121).

Trade secrets, however, are protected under the Electronic Espionage Act of 1996. While no private cause of action is permitted for the trade secret owner whose secret is illegally acquired, the law does enforce criminal penalties for the unauthorized transmittal, downloading, and uploading of trade secrets using computers (Electronic Espionage Act, 1996).

4.6 Insufficient Internal Controls

Ultimately, the loss of the financial benefits of trade secrets stems from mismanagement and the lack of sufficient internal controls. More than half of these breaches occur as a result of corporate mismanagement of the information or from insiders who abuse their access to the information (Rowe, 2007). The burden, then, is on the trade secret owner to establish a "comprehensive trade secret compliance plan" (Pacini et al, 2009, pp. 121). This involves continual assessment of the security systems in place: what additional data must be protected, what information is currently protected, and how information will be protected based on new or developing risks (Cundiff, n.d.).

As in all situations requiring crisis planning, establishing systems to protect data before a breach allows the business to develop a more thoughtful approach to the protection of its trade secrets. The approach must include both the legal and technical aspects surrounding the area of trade secrets. By doing so, when or if a breach occurs, the trade secret owner will have the evidence necessary to establish the efforts maintained to protect the information and hopefully, have the means to identify how the wrongdoer was able to access the information (Green, 2007).

Clearly, the trade secret compliance plan must take the digital environment into consideration and to do that, the trade secret owner must rely on IS professionals to provide the advice and tools needed to protect the trade secret.

5. TEACHING TRADE SECRET LAW TO IS STUDENTS

The study of trade secret law and the important role of IS professionals in protecting the competitive advantage provided by trade secrets provides students with an opportunity to learn new skills and enhance professionalism

through the solution of real-world problems. Constructivism is a form of learning that suits this process well.

5.1 Constructivism

The term "constructivism" covers a broad array of complex philosophical theories that address the way knowledge is acquired (Phillips, 1995). Words alone cannot transfer knowledge; rather, the transfer requires that the learner be engaged in active sensory modes of acquiring knowledge (von Glaserfeld, 1989). A learner processes new information in an active manner with the learner "sensing, acting, and thinking" (Phillips, 1995, pp.11), and constructivism reflects a way of knowing that is active, not passive (Phillips, 1995). The learner is active in the creation, interpretation and reorganization of the new knowledge in a way that is unique to the learner (Windschitl, 1999). This method of processing new information forces the learner to think through new information, resulting in a deeper understanding of that information (Thanasoulas, 2001). While the active construction of knowledge is personal, the developmental process can be triggered by personal or from shared experiences. "Cognitive constructivism" recognizes that learners personally construct ideas based on individual experiences; "social constructivism" expands the construction process to include interaction with others as another means of making sense of new information (Thanasoulas , 2001)

As an epistemology, constructivism focuses on learners. It is not a specific instructional method; instead, various activities place the focus of gaining knowledge on the learner (Schweitzer et al., 2008). Moreover, the social aspect to learning in the constructivist classroom is supported by group work and interaction with the instructor (Powell et al., 2009). The classroom should provide experiential activities that increase knowledge and support deeper understanding (von Glaserfeld, 1989). Hands-on, real-world situations, which are relevant to the student and encourage realistic approaches to solving problems, support the constructivist approach (Johnson, 2009).

Another component of the constructivist classroom calls for group work because peer interaction deepens both the learning process and understanding (Schweitzer et al., 2008). The construction of knowledge is often a cooperative learning experience (Perkins, 1999). In a group setting, members and the problems they address often create cognitive challenges that compel learners to consider the exchanges, process information and ultimately create new knowledge (von Glaserfeld, 1989). Groups also provide diversity as students recognize alternative perspectives by considering how other learners think and process knowledge (Perkins, 1999). Group activities providing alternative perspectives and solutions increase the variety of learning experiences (Powell, et al., 2009). Moreover, group work allows students to observe how others learn and participate in another's thinking process (Windschitl, 1999). In addition, learners are exposed to peers as resources, de-emphasizing the traditional view that the professor is the only resource (Schweitzer et al., 2008).

5.2 Application to IS

The constructivist approach has particular application to the development of skills IS professionals need in their careers. Problem solving, the design and development of systems, and the need to collaborate with others are essential skills for those working in IS (Topi et al., 2010). The IS 2010 guidelines specifically encourage both group activities and real-world, practical exercises to aid students in mastering vital skills (Topi et al., 2010). The exercise below provides IS students with a meaningful reference to legal and technical issues associated with the workplace. Having groups of students develop their own trade secret compliance plan as an active-learning exercise prompts them to think about many of the same data security issues presented in case studies but in the context of a real-world experience.

6. TRADE SECRET EXERCISE FOR IS STUDENTS

The following exercise serves a three-fold purpose. It exposes IS students to legal issues surrounding trade secrets (applicable to other areas of data security), provides student groups with opportunities to apply concepts learned in the classroom, and is conceptual enough to allow instructors the opportunity to set specific parameters, such as the type of deliverable (whether oral or written presentation), among others. The exercise supports team work, collaboration, critical thinking, system analysis, and effective communication skills.

6.1 Information for instructors

This exercise should be completed by students working in teams. It is suggested that the students have a class discussion on trade secrets and the role of IS professionals in securing trade secrets using background information in this paper and other sources to complete the exercise. The exercise could be a long-term project, with additional suggestions for system design and data security as the students advance through their coursework, or the exercise could be a short project to expose students to demands of the IS profession. One possible solution to the exercise, with supporting materials, is available on the JISE's teaching notes which can be accessed by contacting the editor.

6.2 Information for students

6.2.1. Background information: About ten years ago, Jan gave up the work-a-day world to pursue his dream, brewing beer. It had been a hobby for many years and with support of family and friends, he struck out on his own to establish a microbrewery, Smokey Mountain Brews, in a college town. Over the past decade, his business has grown not only with established customers, but also with regional restaurants. Transporting beer, including his signature brew, Smokey Mountain Ale, to surrounding localities, including the city of Asheville, North Carolina, has been time-consuming and expensive. So, two years ago, Jan began planning to open a second brewery in Asheville, a city nationally-known for its microbrews, and those plans are in the final stages. The facility is ready to go, equipment in place, and an assistant brew master hired.

The problem, though, is that Jan is worried about maintaining the confidentiality of his brew recipes. Microbrewing is very competitive and the success of his signature beers equates with the overall success of his brewery. Should his competitors produce a similar brew, his goodwill and market share will drop. His assistant brew

master will have to know the recipes, so the possibility of these recipes getting out has weighed heavily on his mind. To attempt to resolve his concerns, Jan scheduled an appointment with his attorney.

6.2.2. What the lawyer advised regarding acceptable standards of conduct: After explaining his situation to the lawyer, the attorney gave Jan a short overview on options available to protect his recipes: registering a copyright, applying for a patent or maintaining the information as a trade secret. After discussing the pros and cons of each,

Jan and his lawyer determined that the best option was to maintain the information as a trade secret. The lawyer advised on acceptable standards of conduct and told Jan to provide information to employees on a need-to-know basis, to clearly identify confidential information as confidential, to have all employees sign non-disclosure and non-compete agreements, and to talk to his information systems team about establishing some security measures for the data.

6.2.3. What steps have already been taken to secure trade secrets: In accordance with the lawyer's advice, Jan has already taken some steps to ensure the confidentiality of his trade secrets. He has determined who will need to know this information in order to produce the beer and has had both non-disclosure and non-compete agreements drafted by the lawyer for execution by his employees. A procedure for exit interviews has also been developed.

6.2.4. Meeting with IS team: Jan and Rita have worked together on IS issues throughout his brewing career and now that his business is expanding, Jan has put Rita on his staff full time. Jan conveyed the information from the lawyer to Rita and requested that Rita draft an IS compliance plan for digitally securing his recipes. At Rita's suggestion, Jan hired a team of IS professionals to work on a consulting basis to establish the compliance plan.

6.2.5. The plan: Rita and the IS team are doing some background work on issues associated with trade secrets and digital information in an effort to address concerns and create a plan to minimize risks. The plan is due to Jan in just a few weeks so they need to ramp up quickly.

Balancing trade secret value with the cost associated with its security, what should be included in the IS security compliance plan for Jan's trade secrets? What technology can be used to assess risks to the trade secrets? How can access to the information be monitored? What suggestions can the team make to Jan to assist in securing his trade secrets? Why are those suggestions the best for Jan?

7. CONCLUSION

The intersection of law and IS will be one at which IS professionals find themselves throughout their careers. Trade secret law provides an excellent example of how legal and technical issues must be resolved to better serve business and the economy.

IS professionals play a vital role by developing, maintaining, enforcing and auditing the systems and processes required to protect the secrets from security threats. In fact, legal protection of trade secrets is based largely on the efforts the business makes to keep identified information secret. In order to protect trade secrets, companies must demonstrate to the court the reasonableness of the measures they have taken to maintain secrecy. Their success in demonstrating this will determine the extent, whether legal remedies are warranted when a trade secret is wrongfully divulged.

The study of trade secret law from the perspective of the IS staff charged with protecting the data allows students to gain a richer understanding of the nature of the challenges upon entering the workforce. It often comes as a surprise to IS students that success in their careers will require more than just strong technical skills; they will need to understand how the organization works and the environment in which it exists. Learning about the role of IS in protecting trade secrets, as well as the consequences for failing to do so, provides students valuable insights into the complex environment they will face in their careers. Your students need to know how to keep a secret.

8. REFERENCES

Administration's Annual IP Report: IP Related Prosecutions Up, Focus on Health and Safety Redoubled, (2008), Commerce News, Retrieved April 13, 2011 from http://2001-2009.commerce.gov/NewsRoom/PressReleases_FactSheets/PROD01_005190

Ashland Mgt. Inc. v. Janien, (1993) 82 N.Y. 2d 395, 624 N.E. 2d 1007.

Beckerman-Rodau, Andrew. (2002) "Trade Secrets-The New Risks to Trade Secrets Posed by Computerization," Rutgers Computer and Technology Law Journal, Vol. 28, pp. 227-265.

Brenton, Kyle W. (2009) "Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions," University of Illinois Journal of Law, Technology and Policy, pp. 429-475.

Cundiff, Victoria A. (ND), Recent Developments in Trade Secrets Law, Retrieved April 14, 2011 from http://www.ipsectioncolorado.org/content/PowerPoint/CO_Trade_Secrets_Presentation.pdf

Cundiff, Victoria A. (2009) "Reasonable Measures to Protect Trade Secrets in a Digital Environment," IDEA: The Intellectual Property Law Review, Vol. 49, pp. 359-428.

Diamond Power International Inc. v. Davidson, (2007) 540 F. Supp. 2d 1322.

Electronic Espionage Act of 1996, 18 U.S.C. §§ 1831-9.

Ford, Janet, White, Barbara Jo, and Willey, Lorrie (2010) "Software Development and Intellectual Property: What You Don't Know Can Hurt You," Issues in Information Systems, Vol. XI pp. 77-84.

Green, Robert P. and Dickinson, Glenn (2007), Inside Job: without the right IP protection, internal abuse is a fear-inducing threat, Retrieved April 15, 2011 from http://findarticles.com/p/articles/mi_m0ICC/is_1_76/ai_n27325063/

In Re Union Pacific R. Co., (2009) 294 S.W. 3d 589.

Johnson, Genevieve Marie (2009) "Instructionism and Constructivism: Reconciling Two Very Good Ideas," International Journal of Special Education, Vol. 24, No. 3, pp. 90-98.

Lao, Marina (1998) "Federalizing Trade Secrets Law in an Information Economy," Ohio State Law Journal, Vol. 59, pp. 1633-1703.

Legislative Fact Sheet –Trade Secret Act, Uniform Law Commissioners, (n.d.) Retrieved April 12, 2011 from http://www.nccusl.org/LegislativeFactSheet.aspx?title=Trade%20Secrets%20Act

Liebert Corp et al v. Mazur et al, (2005) 357 Ill. App 3d 265.

North Carolina Trade Secret Act, N.C.G.S. §§66-24-152 through 157.

Pacini, Carl and Placid, Raymond (2009) "The Importance of State Trade Secret Laws in Deterring Trade Secret Espionage," Buffalo Intellectual Property Law Journal, Vol. 7, pp. 101-146.

Perkins, David (1999) "The Many Faces of Constructivism," Educational Leadership, Vol. 53, No. 7. pp. 6-11.

Phillips, D.C. (1995) "The Good, the Bad and the Ugly: The Many Faces of Constructivism," Educational Researcher, Vol. 24, No. 7, pp. 5-12.

Posdata Co.. Ltd. v. Kim et al, (2007) 2007 US Dist. LEXIS 48359.

Powell, Katherine C. and Kalina, Cody J. (2009) "Cognitive and Social Constructivism: Developing Tools for an Effective Classroom," Education, Vol. 130, Issue 2, pp. 241-250.

Rockwell Graphic System v. DEV Industries Inc., (1991) 925 F2d 174.

Rowe, Elizabeth A. (2007) "Introducing a Takedown for Trade Secrets on the Internet," Wisconsin Law Review, Vol., pp. 1041-1089.

Rowe, Elizabeth A. (2009) "Contributory Negligence, Technology, and Trade Secrets," George Mason Law Review, Vol. 17, pp. 1-37.

Rowe, Elizabeth A. (2010) "Trade Secrets, Data Security and Employees," Chicago-Kent Law Review, Vol. 84, pp. 749-758.

Schweitzer. Lisa and Stephenson, Max (2008) "Charting the Challenges and Paradoxes of Constructivism: A View from Professional Education," Teaching Higher Education, Vol. 13, Issue 5, pp. 583-593.

Tedder Boat Ramp Systems, Inc. v. Hillsborough County (1999), 54 F. Supp. 2d 1300.

Thanasoulas, Dimitrios (2001) "Constructivist Learning," ELT Newsletter, Retrieved April 1, 2011 from http://www.eltnewsletter.com/back/April2001/art542001.htm

Topi, H., Valachich, J.S., Wright, R.T., Kaiser, K., Nunamaker, Jr., J.F., Sipior, J.C., & de Vreede, G.J. (2010). IS 2010: Curriculum Guidelines for Undergraduate Degree Programs in Information Systems. *Communications of the Association for Information Systems*, Vol. 26, 359-428.

Uniform Trade Secret Act (1985), Retrieved April 1, 2011 from http://www.law.upenn.edu/bll/archives/ulc/fnact99/1980s/utsa85.htm

United States Constitution, Article 1, Section 8.

von Glaserfeld, Ernst (1989) "Cognition, Construction of Knowledge, and Teaching," Synthese , Vol. 80, No. 1, pp. 121-140.

Wiens, Jordan (2007) "Time to Take Action Against Data Loss, "InformationWeek," November 17, 2007, pp. 2.

Windschitl, Mark (1999) "The Challenges of Sustaining a Constructivist Classroom Culture," Phi Delta Kappan, Vol. 80, Issue 10, pp. 751-755.

Yip, Pamela (2006) "Firms ready to put leash on laptops," Dallas News.com, Retrieved April 15, 2011 from http://www.cbiz.com/pdfs/ITN_2006-07-15_Dallas_Morning_News.pdf

AUTHOR BIOGRAPHIES

Lorrie Willey, Assistant Professor of Business Law at Western Carolina University, earned a JD from the University of Tennessee and an EdS from Appalachian State University. Her interests include the application of law and ethics to business practices. Her articles have appeared in Business Law Review, Journal of Legal, Ethical and Regulatory Issues, Entrepreneurial Executive, Journal of Legal Studies Education and Issues in Information Systems.

Janet C. Ford, Assistant Professor of Business Law at Western Carolina University, has a JD of Law from the University of South Carolina. Her interests include constitutional law and workplace privacy issues. Her articles have appeared in the Texas Tech Law Review, Journal of Legal, Ethical and Regulatory Issues, Journal of Financial Service Professionals, Issues in Information Systems.

Barbara Jo White, Associate Professor of Computer Information Systems at Western Carolina University, has a PhD in Business Administration from the University of Mississippi. Her interests include engagement work with IS students and local not-for-profit organizations. A Returned Peace Corps Volunteer, she has published manuals with Peace Corps and had articles appear in Decision Sciences Journal of Innovative Education, Issues in Information Systems, Small Group Research, Computers & Operations Research, Mountain Rise, Leadership and Organizational Development Journal and Business Communication Quarterly.

Danial L. Clapper, Associate Professor of Computer Information Systems at Western Carolina University, has a PhD in Decision Sciences from Georgia State University. His interests include mobile web application development and small business security. His research has been published in the Journal of the International Academy for Case Studies, Journal of Strategic E-Commerce, and Academic Exchange Quarterly.

Information Systems & Computing
Academic Professionals

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the Journal of Information Systems Education have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN 1055-3096