Data Security and Privacy: Into the Breach

Martha Lessman Katz, JD, CIPP, CLP

Martha Lessman Katz, JD, CIPP, CLP, is a principal at Miles & Stockbridge PC in Baltimore, Maryland.

In 2007, an attack against the computer systems of the TJX Co. potentially exposed credit card and other personal information of 45 million T.J. Maxx customers. The 2008 intrusion into Heartland Payment Systems' processing system—the fifth largest in the United States[1]—compromised more than 100 million credit and debit card transactions. And in an ignominious end to 2009, a malicious attack against RockYou.com's user database compromised the user names, passwords, and e-mail addresses of more than 32 million accountholders.

Stolen confidential business and personal information may be disseminated over the Internet in a matter of minutes. Even if personal data are not compromised, the loss of even one computer may mire an institution in a tangled web of international data security and privacy laws and regulations. And the resulting financial cost pales when compared to the damage to reputation, customer wrath, and loss of trust.[2] Still, rarely a day goes by without a data breach being reported by an academic institution, health-care organization, or other business or government agency.

Data breaches increased as much as 47 percent in 2008, exposing as many as 35 million records.[3] While academic, governmental, and military institutions reported a decrease in breaches, business breaches climbed from 21 percent to 41 percent between 2006 and 2009.[4] Still, breaches continue to be reported by organizations of all types. For example, it was reported that:

- Binghampton University in New York kept information for every student, possibly dating back at least 10 years, in a storage room next to one of the most heavily trafficked lecture halls on campus. The storeroom door was taped open to prevent it from locking. The information, which included Social Security numbers, credit card numbers, scans

©2010 Association of University Technology Managers and chapter authors named above. All rights reserved. Reproduction in whole or in part without written consent of the copyright owners is prohibited. Contact AUTM regarding reuse of any part of this work. Opinions expressed in this publication by authors are their own and do not necessarily reflect the opinions of AUTM or the organizations with whom the authors are affiliated.

of tax forms, employee salary and immigration asylum information, was disorganized and haphazardly maintained in boxes sprawled throughout the two-story room and in unlocked filing cabinets.[5]

- The University of Hawaii notified people who conducted business with one of its parking offices for 13 years that an unauthorized access to its database server occurred on May 30, 2010. Of the 53,000 affected records, 41,000 Social Security numbers and 200 credit card numbers were exposed.
- University of Florida officials notified more than 2,000 people that in May 2010 their Social Security or medical identification numbers were included on address labels affixed to letters mailed through the U.S. Postal Service, inviting them to participate in a research study. The same information was also shared with a telephone survey company.
- The compromise of a University of Maine database exposed names, Social Security numbers, and medical information of every student who visited the university's counseling service between 2002 and 2010.[6]

Contrary to common thought, the overwhelming majority of breaches results from information mishandling or insufficient (or failing to follow) privacy processes and procedures, not cyber attacks or hackers. For instance, simply wiping data from a defective hard drive returned to its vendor for repair would have prevented the breach of up to 76 million records about U.S. military veterans, including Social Security numbers dating as far back as 1972.[7] Studies indicate that of all reported breaches for 2008, only 2.4 percent of the data were encrypted or secured by other strong protection mechanisms (decreasing to 1 percent in 2009[8]), and only 8.5 percent of the data were even password protected.[9]

Social Security numbers of several hundred alumnae of Armstrong Atlantic State University's nursing school were compromised when a portable hard drive was stolen from the campus, despite the fact that use of portable devices to store confidential information violated university policy.[10] Historically, institutions have spent more on cyber security prevention although, until very recently, only a small percentage of breaches occur as a result of malicious attacks.

©2010 Association of University Technology Managers

Malicious attacks exceeded human error for the first time in 2009, with hackers and insider theft accounting for 36.4 percent of all breaches and human error accounting for 27.5 percent,[11] a trend that continued in 2010 with hacking accounting for 17.1 percent and insider theft at 15.4 percent.[12] While the total number of reported breaches declined in 2009, 60 percent of those reported represented system breaches affecting almost 222.5 million records.[13] And, although academic and health-care organizations generally have experienced fewer breaches than their commercial counterparts, it may be due more to kismet than conscious choice.

Indeed, their exposure risk is exceedingly high in light of the sensitivity of the collected data. And yet, a 2009 survey found that while 98 percent of health-care organizations have implemented information security and privacy policies, fewer than half use encryption or data anonymization technology.[14] What will it take for U.S. organizations[15] to make data security as second nature as issuing identification cards/security badges and locking their doors? And what role should technology transfer managers play with respect to data security and privacy issues?

An overview of privacy and data security basics follows, distinguishing the laws of Canada and the European Union (EU) from those of the United States. This overview will illustrate the differing approaches and cross-border privacy issues confronting academic institutions with respect to their faculty; students generally and in connection with clinical trials and other research; health-care providers with respect to their patients; and all organizations with respect to their existing and prospective customers, employees, and suppliers.

Canada and the EU treat privacy of personal information as a fundamental human right to be controlled by the individual and, therefore, address security and disclosure of private information through comprehensive laws and regulations. Canada protects the privacy of its residents through its Personal Information Protection and Electronic Documents Act (PIPEDA).[16] The EU governs protection, processing, sharing, and transborder flows of personal data through the EU Privacy Directive, which directs each EU member state to enact its own local law. The EU Directive serves as a blueprint for each member state's local privacy statutes, most of which are enforced through each member state's Data Protection Authority.[17]

©2010 Association of University Technology Managers

Neither Canada nor the EU Privacy Directive permits use or sharing of personal information without first obtaining the subject individual's explicit and informed consent and providing individuals with the ability to access and update their data and a complaint process. The information must also be used or disclosed only for the purposes for which it was collected. This is commonly referred to as the *opt-in approach.*

Canada, the EU, and its individual member states aggressively and proactively protect individual privacy.[18] Although it was originally thought that Canada's PIPEDA only applied to entities having a physical presence in Canada, a 2007 court decision held otherwise. In *Lawson v. Accusearch Inc.*,[19] the Federal Court of Canada determined that Canada's Office of the Privacy Commissioner (OPC) had the authority to investigate complaints against businesses that collect, use, or sell personal information of Canadians, even if the entities have no physical infrastructure within Canada. The EU and its members have also determined that its data protection legislation applies to social networking site operators, even if their headquarters are not located in the EU.

Similarly, the EU Privacy Directive has been expansively interpreted by the Article 29 Data Protection Working Party (Working Party), applying EU data protection law to non-EU Web sites that set cookies or use JavaScript that runs on their residents' computers.[20] This position was reaffirmed by the Working Party's opinion on search engines, endorsing the view that an Internet protocol (IP) address or unique cookie identifier, in and of itself, may be personal data and reiterating that setting cookies or other activities locally on a user's PC is sufficient to trigger applicability of EU data protection law, as is having ad sales in connection with the search engine.[21] Having a local office, local customer support, or a third-party agent within a member state would also suffice.

Online advertisers are finding that their behavioral targeting practices are being closely scrutinized. An amendment to the EU's Privacy Directive requires that consumers give prior, explicit consent before cookies may be placed on the computers of EU residents. The U.S. Federal Trade Commission (FTC) issued its Self-Regulatory Principles for Online Behavioral Advertising[22] providing for transparency, consumer control, and reasonable security for consumer data similar to the EU requirements, exhorting companies to use the principles as a catalyst to developing industrywide self-regulatory practices.

©2010 Association of University Technology Managers

In response to high-profile data breaches by EU companies, EU members continually address gaps in their laws. For example, Germany's Data Protection Act has been expanded to reach to all collection, processing, and use of personal data, requiring that personal data be anonymized unless cost prohibitive and that, absent an existing relationship, marketing and research firms obtain consumer permission to use even address data. Germany has also introduced U.S.-style data breach notification obligations, the one area in which the EU still lags behind the United States.[23]

Having undergone a five-year review in 2010, Canada's PIPEDA was amended in 2010 to include breach notification to the OPC and affected individuals, enforcement of which began immediately. (The FTC's efforts to align the interests of the United States and the EU generally and in connection with behavioral advertising and data breach notification laws of individual states are discussed more fully below.)

Additional examples of aggressive regulation outside the United States include the Scottish government's Identity Management and Privacy Principles for public service organizations aimed at increasing public confidence in the handling of private data, including guidance on identity verification, audit trails, data sharing, and risk management.[24] Canada's OPC required that Bell Canada make more transparent its practice of using deep-packet inspection technology to tie users' online activities to their IP addresses.[25]

Facebook found itself in the crosshairs of the OPC and privacy advocates when modifications to its privacy policy made information located on user pages more available. In response, Facebook implemented safeguards designed to better protect the personal information of its users and their online friends on deactivation and from third parties, such as application developers.[26] And, citing the failure of social networking sites to adequately protect user data as reflected in their online privacy statements, Germany's data protection commissioner has proposed an independent ratings agency to alert users to the risks of the various social networking Web sites.

Proximity and more familiarity with language and culture often lead U.S. businesses to test the global market by expanding internationally to Canada first and then to the EU. But Canada's comprehensive framework is not the approach taken by U.S. privacy laws and regulations. The Privacy Act of 1974[27] regulates the collection and use of records by

©2010 Association of University Technology Managers

U.S. federal agencies and affords individuals the right to access and correct their personal information. Information disclosed for any "routine use" compatible with the agency's purpose in collecting the information is excluded. The law does not apply to state and local agencies or the private sector.

In contrast to the broad umbrella approach to data security and privacy reflected by EU and Canadian law, no overarching U.S. federal law governs the private sector's use and protection of personal information.[28] Rather, in addition to endorsing industry self-regulation through technology and privacy statements (the *opt-out standard*), to date the U.S. government has approached privacy from an information use/sector-specific perspective, focusing on information misuse. As a result, federal data security and privacy laws in the United States have developed in patchwork fashion, geared toward the regulation of targeted types and uses of information, i.e., consumer credit information,[29] health and medical information,[30] financial information,[31] personal information of children,[32] driver's license information,[33] and e-mail.[34] A law even protects against disclosure of video rental information. [35]

That said, the U.S. privacy approach is shifting. Following public hearings and roundtable discussions on consumer privacy, in December 2010, the FTC proposed a comprehensive framework for protecting personal information, including a privacy-by-design approach through which organizations would build privacy protections into their everyday business practices.[36] Believing the advertising industry's self-regulatory efforts to support transparency and choice—as set forth in its Self Regulation Principles discussed above—have fallen short, the FTC included a do-not-track program for online advertising, advocating a uniform, comprehensive choice mechanism such as a persistent cookie-like browser setting through which consumers would be able to choose whether to allow the collection and use of data regarding their online searching and browsing activities. The consumer's selected settings would be conveyed to sites visited by the consumer's browser to signal whether or not the consumer has consented to be tracked or receive targeted advertisements. In response, Microsoft announced[37] it will include functionality in its Internet Explorer Web browser that would limit the ability of advertisers and analytics providers to collect and use a user's online browsing data.

©2010 Association of University Technology Managers

On the heels of the FTC's issuance of its proposed framework, the Department of Commerce issued its policy recommendations for promoting online privacy that include the creation of a Department of Commerce National Program Office to coordinate federal activities needed to implement the National Strategy for Trusted Identities in Cyberspace.[38]

Many U.S. states, following the same informal/sector-specific approach, stepped into the chasm created by the lack of comprehensive federal legislation by regulating consumer credit, driver's license, Social Security, supermarket club, and credit card information. In 2000, California set the gold standard by establishing the Office of Privacy Protection within its Department of Consumer Affairs. From then on, California statutes have served as the foundation for a proliferation of laws enacted by a majority of states, mandating that policies be implemented to secure information to prevent unauthorized use and identity theft and recommending action to be taken in the event of a data breach.

A New York statute, enacted in 2009, prohibits employers from posting, displaying, or otherwise communicating personally identifiable information of employees, such as Social Security numbers, home addresses, telephone numbers, or e-mail addresses to the general public.[39] Massachusetts enacted a first-of-its-kind data security law requiring that businesses not only develop and maintain a security program with administrative, technical, and physical safeguards for personal records, but also encrypt all personal information transmitted wirelessly, stored on laptops or other portable devices, and, if feasible, personal information transmitted across public networks. All businesses that own, license, store, or maintain personal information about a Massachusetts resident, regardless of whether that organization is itself present in the state, must comply.[40] Until the U.S. Congress enacted the Health Information Technology for Clinical Health Act (HITECH) in 2009,[41] the first significant national reporting statute, California's laws obligating health organizations to safeguard patient data and its state enforcement office provided the most comprehensive protection of patient data.[42]

Although U.S. state laws vary in their specifics, they generally require that organizations (1) protect personal information from unauthorized access, use, modification, or disclosure; (2) maintain reasonable security procedures appropriate to the nature of the personal information and the nature and size of the organizations and their operations; (3)

©2010 Association of University Technology Managers

destroy records containing personal data under certain circumstances to prevent inappropriate access; (4) mandate in writing that their third-party service providers implement appropriate procedures in compliance with law; and (5) take certain action upon learning of a personal data breach, including prompt notice to affected individuals, law enforcement, and consumer credit-reporting agencies. Violations of state statutes tend to be characterized as unfair or deceptive practices subject to civil and criminal penalties.

With the exception of the individual states' data breach notification laws, protections afforded U.S. residents by law and the opt-out approach fall short of those afforded to residents of the EU. As a result, the EU restricts the flow of its residents' personal data to the U.S., absent the recipient's compliance with *adequate* privacy laws or explicit consent by the individual. In an effort to bridge the differing approaches to privacy and data security, the U.S. Department of Commerce, in consultation with the European Commission, developed a safe-harbor framework.

By complying with the following seven principles, organizations may avoid prosecution by European authorities under European privacy laws:

1. Individuals must be advised of the purpose for which the information is being collected, to whom it may be disclosed, how to restrict use and disclosure, and how to address inquiries and complaints.
2. Individuals must be given the opportunity to consent to disclosure of their personal data to a third party or use in a manner other than that for which it was initially collected.
3. The notice and choice principles (items 1 and 2 above) must be applied before disclosing information to third parties. Third-party service providers should be required in writing to comply with EU privacy protection principles.
4. Individuals must be able to access their information to correct, amend, or delete it.
5. Reasonable precautions must be taken to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction. This would include reasonable steps to ensure that data is accurate, complete, current, and reliable for its intended use.
6. Personal information collected must be relevant to the purpose for which it is collected.
7. Finally, procedures should be implemented to verify compliance and investigate and resolve complaints.

©2010 Association of University Technology Managers

In an effort to move the U.S. toward a more unified approach, the FTC developed its Fair Information Practice Principles, a collection of reports, model codes, and guidelines with common core principles that more closely match EU requirements. These include: (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress.[43] And to address the burgeoning problem of misuse and loss of personal information, the FTC[44] developed additional rules and safe-harbor guidelines, including the creation of its Division of Privacy and Identity Protection, to assist the private sector in its efforts to protect personal data and comply with the varying federal data protection statutes.[45]

For example, the FTC's Financial Privacy Rule requires that financial institutions give clear privacy notices explaining their privacy and data-sharing policies and disclose to their customers how to limit information sharing, i.e., how to opt out. If a consumer does not opt out, then his or her personal data may not only be used by the financial institutions but also by his or her third-party service providers with which it is shared, including further disclosure if permitted by the financial institution's privacy policy.

The FTC's Safeguards Rule obligates companies subject to the Graham-Leach-Bliley Financial Services Modernization Act (G-L-B) [46] to have and implement written security plans appropriate to their size and complexity, the nature and scope of its activities, and the sensitivity of the information being handled to protect the confidentiality and integrity of personal information collected. The Safeguards Rule requires that businesses designate a plan coordinator to identify and assess risks to information in each area of operations; evaluate the effectiveness of current safeguards; design, implement, monitor, and regularly test the efficacy of the plan; and evaluate and adjust the plan in light of not only the test results but also changes in business operations and other relevant circumstances.

The FTC's Disposal Rule requires that businesses take reasonable steps to prevent unauthorized access to or use of sensitive information derived from consumer reports and to properly dispose of it (e.g., by shredding, burning, destroying electronic media, etc.). The Disposal Rule applies to not only consumer reports but also information derived from consumer reports (such as credit scores, background information, insurance claims, check writing, and medical history). The FTC encourages those who dispose of *any* records

©2010 Association of University Technology Managers

containing personal or financial information to take similar measures, taking the position that *anyone* accessing consumer reports for business purposes, not just those subject to G-L-B, is subject to the FTC Disposal Rule. In view of this, the Disposal Rule casts a much wider net, ensnaring less sophisticated users such as landlords, automobile agencies, personnel departments, and even families seeking nannies or other household help.

The FTC's standard for information security recognizes that information collected by organizations varies widely in its sensitivity, requiring only that reasonable procedures to protect sensitive information are maintained based on the nature and size of the organization, its resources, type and sensitivity of information collected, etc. The following are of particular import to the FTC with respect to compliance with its information security rules.

- Employee management and training
  -- Background/reference checks
  -- Employee buy-in via written agreements
  -- Limiting access to those with a need to access
  -- Controlling access via strong passwords that are regularly changed
  -- Password-activated screen savers that lock computers after a period of inactivity
  -- Policies addressing use of portable equipment such as laptops, personal digital assistants, or other remote devices capable of storing information
  -- Training employees to lock sensitive data, not share passwords, encrypt sensitive information, and report suspicious activity
- Information systems (include network and software design, information processing, storage, transmission, retrieval, and disposal)
  -- Ensure protection against physical hazards such as floods and fires.
  -- Store tangible sensitive data and/or the equipment housing the data in locked rooms.
  -- Back up records and archive off site.
  -- Avoid storing sensitive data on the Internet.
  -- Encrypt sensitive data for storage and transmission.
  -- Properly dispose of sensitive information.
- Deter, detect, defend: Detection and management of system failures
  -- Keep abreast of emerging threats and defenses.
  -- Keep systems/programs up to date via patches, antivirus software, firewalls, intrusion detection, and logs.

©2010 Association of University Technology Managers

-- Keep employees informed of risks and possible breaches.
-- Develop and implement oversight and audit procedures, i.e., monitoring in-bound and out-bound transfers, create dummy accounts to detect unauthorized hits.
-- Retain security professionals to test/stress security.

- Notify affected individuals, law enforcement, and related businesses in the event of a security breach.

Taking its cue from the recommendations of the 2006 Identity Theft Task Force and in an effort to address the increase in identity theft and discrepancies under the Fair and Accurate Credit Transactions Act of 2003,[47] the FTC and other federal regulatory agencies enacted the Red Flags Rule. The Red Flags Rule requires that financial institutions and creditors holding any consumer account (or other account for which there is a reasonably foreseeable risk of identity theft) develop and implement an identity theft prevention program by December 31, 2010.[48] Programs must identify and detect activities that may be red flags signaling possible identity theft and implement procedures to respond accordingly.

Who is subject to the Red Flags Rule? Any financial institution or *creditor* that offers one or more covered accounts must comply. Any entity extending credit to its customers is a creditor and may have consumer accounts subject to the rule. A creditor includes any entity that regularly defers payment for goods or services or provides goods or services and subsequently bills the recipient. It is an organization's *activities* and not its industry or sector that determines if it is a creditor subject to the rule. Therefore, academic institutions, health-care providers, and telecommunications companies may fall within the definition, depending on how and when they collect payment for services. Those who regularly grant or arrange for loans or the extension of credit or make credit decisions may meet the definition of a creditor. Anyone offering financing or assisting in the acquisition of financing from others, i.e., processing credit applications, are also included.

Current FTC guidelines[49] describe two relevant forms of covered accounts: (1) consumer accounts designed to permit multiple payments or transactions and (2) any other account that a creditor offers or maintains for which there is a reasonably foreseeable risk of identity theft to customers or to the safety and soundness of the creditor, including financial, operational, compliance, reputation, or litigation risks. Academic institutions maintain covered accounts through bookstore accounts, tuition and other financial accounts,

©2010 Association of University Technology Managers

employment applications, patient accounts (if not covered under the Health Insurance Portability and Accountability Act (HIPAA)), student and employee accounts receivable, parking offices, and the like.

In determining foreseeability, the FTC recommends that businesses consider how accounts are opened and accessed. The ability to remotely access the account may create a reasonably foreseeable risk of identity theft. Companies are also advised to consider any actual incidents of identity theft they have experienced involving such accounts. Because the test cited in item 2 above includes a determination of the reasonable foreseeability of identity theft, it requires an assessment of the extent and effectiveness of an organization's privacy and data security policies, practices, and procedures.

Covered entities must implement an identity theft program, conduct ongoing risk assessments, and regularly update their policies and training programs to reflect risk changes based on changes in their business processes, structures, etc., and the ever continuing sophistication of thieves and malware technology. Users of consumer reports must also develop reasonable policies and procedures to apply when they receive a notice-of-address discrepancy from a consumer-reporting agency.

Similarly, HITECH requires prompt notification of breaches of unsecured protected health information. The Department of Health and Human Services reported that between September 2009 and December 2010, health-care organizations suffered serious breaches of more than 6 million patient medical records necessitating the public reporting required by HITECH. The majority of these failures, including one involving almost 1 million records, resulted from simple, preventable security lapses such as stolen disks or laptops, not complex criminal schemes.[50]

At-risk organizations, such as academic institutions, their research sponsors, clinical trial teams, clinical/contract research organizations, and technology transfer licensees (especially those in the life sciences and pharma industries), must be keenly aware of and address privacy and data security issues generally, but especially before engaging in any clinical trial activities. Indeed, even use of digital photocopiers jeopardizes the security of sensitive information if steps are not taken to protect the data stored on the hard drives from remote access, misuse, or innocent disclosure when the photocopiers are retired

©2010 Association of University Technology Managers

from service. Acquisition of data of U.S. and foreign participants, sharing data among all interested parties, and safe storage and destruction must all be considered.

Consequently, all at-risk institutions must seriously consider and enact privacy security standards sufficient to safeguard personal medical data amassed during clinical trials and ensure that their third-party vendors, such as patient recruitment firms, have these capabilities. Medical data acquired in a clinical trial context creates complex privacy issues, requiring that the privacy rights of participants and research-and-information-access needs of trial sponsors and clinicians be sensitively balanced.

Safeguarding the collection, sharing, use, and storage of this sensitive information is as critical to the success or failure of a trial as other variables or events. As technology transfer managers continue to develop and expand the roles they, as agents of academic institutions, play in technology commercialization and startup activities, educating and monitoring their licensee performance in critical at-risk areas, such as data security and privacy, assumes greater importance.

Conclusion

More than ever before, academic and health-care institutions and businesses must not only be aware of the data collection, use, and privacy requirements of each jurisdiction in which they transact business or otherwise operate, but also prepare themselves for the challenges accompanying the inevitable data security breach. Academic institutions must safeguard not only faculty, student, and employee information, but also be keenly aware of HIPAA and the new HITECH rules to protect patient information in the context of research and clinical trials.

General counsel of these institutions address these issues every day as evidenced by the recent data security breaches at the universities of Hawaii, Florida, and Maine, previously discussed. University medical centers also face these issues not just with respect to patient information but also in connection with the conversion to electronic medical records required by HITECH. Many faculty and students of U.S.-based academic institutions are not U.S. residents. Many academic medical centers treat international patients both in the U.S. and international satellite facilities. Moreover, the success of university-industry relationships and technology transfer spin-outs depends, in no small measure, on ensur-

©2010 Association of University Technology Managers

ing that all parties understand and comply with privacy laws. Technology transfer departments are in an excellent position to educate their constituencies in this regard. Existing FTC, Commerce Department safe harbor and other agency rules, existing and proposed U.S. federal and state legislation governing the handling of personal information, as well as actions in the event of a security breach are clearly trending toward the EU model.

While the FTC's Red Flags Rule may not universally apply, U.S. state and international data protection laws do apply to entities if the personal data of their residents are affected by the entities' activities. In the event of a data breach, the notification requirements of each state (and more and more EU countries) apply even if the business is not in violation of law. Moreover, if a business must respond to a personal data breach, a court or regulator's determination that the business's actions are reasonable under the circumstances and the fines imposed may very well hinge on whether the business has policies and procedures in place—probably procedures similar to those mandated by the FTC generally and its Red Flags Rule.

To respond effectively to data breaches, all entities need significant preparation, processes, and systems that enable rapid identification and notification of the breach. The day an organization detects a breach is not the time to begin development and implementation of a plan. Responding to news media, regulatory bodies, and the public is time-consuming, resource intensive, and requires serious attention. It requires risk-based management decisions that should not be made in the heat of the moment or by untrained, untested personnel.

The costs of a security breach, in revenue, personnel resources, and expense, as well as loss of reputation, are far too great to ignore. That a breach will occur is certain. Organizations that meet, rather than ignore, the challenges of securing data save in the long run, on their bottom line, in preservation of good will, and most importantly, by retaining the trust of their faculty, students, patients, employees, and customers. Technology transfer managers are uniquely positioned to assist their employers and constituents with their privacy and data security compliance.

©2010 Association of University Technology Managers

Notes

1. The Nilson Report, Issue 922, March 2009.
2. Under a January 2010 settlement between Heartland and VISA, subject to certain conditions, issuers of Visa-branded credit and debit cards may recover losses incurred up to $60 million. Under a separate December 2009 settlement of consumer cardholder class action suits, Heartland agreed to pay a minimum of $1 million up to a maximum of $2.4 million to class members submitting valid claims. Pursuant to a separate December 2009 settlement with American Express, Heartland agreed to pay $3,538,380 to satisfy issuer losses. Several additional security holder class action suits are pending against Heartland.
3. Identity Theft Resource Center (ITRC), 2008 Data Breach Report.
4. ITRC 2009 Breach Synopsis and Report (January 8, 2010).
5. ITRC 2011 Breach Report List.
6. ITRC July 6, 2010 Breach Report List.
7. ITRC 2011 Breach Report List, supra note 4.
8. ITRC 2009 Breach Synopsis and Report, supra note 3.
9. ITRC 2008 Breach Report, supra note 2.
10. ITRC 2011 Breach Report, supra note 4.
11. ITRC 2009 Data Breach Report, January 2010.
12. ITRC 2010 Synopsis and Report (January 3, 2011).
13. ITRC 2009 Data Breach Report, supra note 10.
14. "Are Hospitals Ready for Meaningful use of EHRS?," *Computer Sciences Corporation Survey,* December 2009, Erica Drazen, and supra note 9.
15. References to *businesses* include academic and health-care institutions.
16. Personal Information Protection and Electronic Documents Act, R.S.C., ch. 5 (Can.), Effective January 1, 2001.
17. European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. EU Directive 95/46 EC of the European Parliament and the Council of 24 October 1995, 1995 O.J. (L 281) 31 at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
18. The UK's Information Commissioner's Office has been authorized to impose fines of up to £500,000 beginning April 6, 2010.

©2010 Association of University Technology Managers

19. *Lawson v. Accusearch Inc.*, 2007 F.C. 125 (Can.)
20. Article 29 Data Protection Working Party Document (May 30, 2002) (WP56), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp56_en.pdf.
21. Article 29 Data Protection Working Party Opinion 1/2008 (April 4, 2008) (WP 148), at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf.
22. See http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.
23. See German Protection Act (BDSG) Section 42a.
24. See http://www.scotland.gov.uk/Publications/2010/12/PrivacyPrinciples.
25. See Personal Information Protection and Electronic Documents Act (PIPEDA) Case Summary 2009-010, http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm.
26. See Personal Information Protection and Electronic Documents Act (PIPEDA) Case Summary 2009-08, http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm.
27. 5 U.S.C. § 552(a).
28. Online consumer data privacy issues are being discussed at the U.S. federal level, and bills introduced to Congress in 2011 may move the U.S. toward comprehensive federal privacy legislation.
29. See Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. (1971) as amended by the Fair and Accurate Credit Transactions Act of 2003 (FACTA) Public Law 108-159.
30. See Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, amending 42 U.S.C. § 1301 et seq. (1996) (HIPAA).
31. See Graham-Leach-Bliley Financial Services Modernization Act of 1999, 15 U.S.C. § 6801 et seq. (1999).
32. See Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 et seq. (1999).
33. See Drivers Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq. (1994).
34. See Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2721 et seq. (1994).
35. See Video Protection Act of 1988, 18 U.S.C. §§ 2710-11.
36. Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers. Preliminary FTC Staff Report, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.
37. See http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx.
38. Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework. The Department of Commerce: Internet Policy Task Force, December 16, 2010, http://ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

©2010 Association of University Technology Managers

39. N.Y. Lab.Law Art 7 § 203-d.
40. M.G.L. c 93H as regulated by 201 CMR 17.00 effective March 1, 2010.
41. The Health Information Technology or Economic & Clinical Health Act amendment to HIPAA was enacted in 2009 as part of economic stimulus legislation, specifically the American Recovery & Reinvestment Act of 2009, Pub.L.No. 111-5, §13421, 123 Stat. 115, 276 (to be codified at 42 U.S.C. §17951).
42. U.S. Senator John Kerry (D. Mass) has introduced legislation in the 112th Congress to establish a federal regulation framework for the comprehensive protection of individuals' personal data following the framework suggested by the FTC.
43. FTC Fair Information Practice Principles, at http://www.ftc.gov/reports/privacy3/fairinfo.shtm.
44. The FTC authority under its charter to prohibit unfair and deceptive trade practices.
45. For example, the FTC's Financial Privacy, Safeguards and Disposal Rules, the Children's Online Privacy Protection Rule: Safe Harbor Program.
46. Supra note 23.
47. See FACTA, supra note 18, which amended the Fair Credit Reporting Act.
48. The FTC delayed to December 31, 2010, enforcement of the Red Flags Rule to enable Congress to issue clarifying legislation. It has also agreed not to enforce the rule on members of the American Medical Association and other professional organizations while their lawsuits, asserting that the inclusion of attorneys and physicians and other professionals within the definition of creditor is too broad, wend their way through the courts.
49. See http://www.ftc.gov/opa/2007/10/redflag.shtm. See also http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf.
50. See Report of Office of Civil Rights of the Department of Health and Human Services at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

©2010 Association of University Technology Managers