Revitalizing Data Stewardship through Risk Reduction: Managing Sensitive Data at the University of Virginia

Bob Albrecht, ECAR
Judith A. Pirani, ECAR

ECAR Case Study 8, 2009

Case Study from the EDUCAUSE Center for Applied Research
Revitalizing Data Stewardship through Risk Reduction: Managing Sensitive Data at the University of Virginia
EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology.

The mission of the EDUCAUSE Center for Applied Research is to foster better decision making by conducting and disseminating research and analysis about the role and implications of information technology in higher education. ECAR will systematically address many of the challenges brought more sharply into focus by information technologies.

Copyright 2009 EDUCAUSE. All rights reserved. This ECAR case study is proprietary and intended for use only by subscribers and those who have purchased this study. Reproduction, or distribution of ECAR case studies to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior written permission is granted by EDUCAUSE. Requests for permission to reprint or distribute should be sent to ecar@educause.edu.
Revitalizing Data Stewardship through Risk Reduction: Managing Sensitive Data at the University of Virginia

Preface

The EDUCAUSE Center for Applied Research (ECAR) produces research to promote effective decisions regarding the selection, development, deployment, management, socialization, and use of information technologies in higher education. ECAR research includes

- research bulletins—short summary analyses of key information technology (IT) issues;
- research studies—in-depth applied research on complex and consequential technologies and practices;
- case studies—institution-specific reports designed to exemplify important themes, trends, and experiences in the management of IT investments and activities;
- roadmaps—designed to help senior executives quickly grasp the core of important technology issues; and
- key findings—brief high-level summaries on the scope of an ECAR research study.

As part of its 2009 research agenda, ECAR recently published a study, Institutional Data Management in Higher Education, by Ronald Yanosky. The study examines how higher education institutions are facing the challenges of institutional data management in terms of quality, stewardship and governance, analytics, content and records management, and research data management.

Literature Review

The literature review helped identify and clarify issues, suggest hypotheses for testing, and provide supportive secondary evidence. Besides examining articles and studies from journalistic, academic, and IT practitioner sources, we consulted with practicing CIOs and data management experts to develop study objectives and survey questions.

Online Survey

We designed and administered a web-based survey that was distributed to institutional representatives (mostly senior IT leaders) at 1,733 EDUCAUSE member institutions in February 2009. We received 309 responses (a 17.8% response rate).

Interviews

We conducted follow-up telephone interviews with 23 senior IT leaders and staff from a mix of institutions to gain deeper insights into findings from the quantitative analysis and to capture additional ideas and viewpoints.

©2009 EDUCAUSE. Reproduction by permission only.
Case Study

ECAR researchers conducted this in-depth case study to complement the core study. We assume readers of this case study will also read the primary study, which provides a general context for the individual case study findings. We undertook this case study of the University of Virginia to study the institution’s multi-layered strategy to resolve practical sensitive-data issues, which in turn revitalized its data stewardship efforts. ECAR owes a debt of gratitude for their time and insights to Susan Barr, Student System Project Director; Brian Davis, Associate Director, Information Security, Policy, and Records Office; James Hilton, Vice President and CIO; Steve Kimata, Assistant VP for Finance and University Comptroller; Valerie Larsen, Center for Instructional Technology Director; Wayne Martin, Medical Center Information Security Manager; Shirley Payne, Assistant VP for Information Security, Policy, and Records Office; Leonard Sandridge, Executive Vice President and COO; and Caroline Walters, University Records Officer.

Introduction

Incidences of institutional data continue to proliferate at an astonishing rate at many colleges and universities, fostered in part by technology. ERP and online systems make it increasingly easy for staff members to weave institutional data into business and academic processes, while personal computing devices like laptops, netbooks, and smartphones facilitate access anytime and anywhere. Today’s storage media, like thumbnail-sized key disks, can collect more data in a few seconds than a fleet of photocopiers could reproduce in a year. All these factors make the care of institutional data an increasingly vital and complicated process, requiring policies and processes to ensure security, accuracy, and timeliness, as well as accessibility and readability—all of which are conceptualized sometimes under the name stewardship. Institutional data’s broad deployment and wide-ranging custodial responsibilities create an environment that requires institutional commitment and involvement.

The University of Virginia (U.Va.) has tackled such issues diligently and collectively since 2007. At that time, the university used Social Security numbers (SSNs) as the personal identifier in its aging student information system and in many of its business processes. “For example, U.Va. still used a previously considered best practice—posting grades using the last four digits of a student’s SSN—to protect confidentiality,” said James Hilton, vice president and CIO. “But in the age of the Internet, this had morphed into a worst practice.” Compounding the situation was a conservative archiving practice that encouraged faculty and staff to become “data pack rats, hoarding institutional data and records” that contained SSNs and other highly sensitive institutional data for years, and in some cases decades, past their usefulness. The result was an institutional environment awash in unnecessary and “unprotected uses of highly sensitive data, creating undue risk” to the university. To rectify the situation, U.Va. launched a multifaceted program that remediates past data usage practices, creates an updated data policy framework, educates the U.Va. community about sound data handling practices, and better protects university data by strengthening the IT infrastructure security.

The key to the success of this program lies with total institutional engagement, from the senior administration to individuals in academic and business departments. The eradication of non-essential, but highly sensitive, data and the compliance with new university data-related policies required intensive local involvement. Departments had to locate and inventory highly sensitive data and, in many cases, then modify long-standing business practices and processes. It required an extensive investment of time, and it sometimes disrupted day-to-day operations.
Today’s result is a transformed university environment with a heightened sense of data stewardship, one that minimizes the use of highly sensitive data and stores it more securely—and most importantly, one that now confronts data management issues proactively rather than reactively. Data management and stewardship at U.Va. have become an institutional effort led centrally and accepted by the university community. This case study details the university’s multi-layered program and studies its repercussions on a cross section of university areas.

**Background**

Founded by Thomas Jefferson in 1819, the University of Virginia is a public research university located in Charlottesville. Approximately 21,000 students attended U.Va. during 2008–2009. The faculty consists of almost 2,200 full-time members, and the university employs more than 10,200 full-time staff members. U.Va. is made up of 12 schools in Charlottesville, plus the College at Wise in southwest Virginia. The university offers 51 bachelor’s degrees in 47 fields, 84 master’s degrees in 67 fields, 6 educational specialist degrees, 2 first-professional degrees (law and medicine), and 57 doctoral degrees in 55 fields. Sponsored research awards totaled more than $314 million for FY 2008.

Hilton, U.Va.’s vice president and CIO, reports to the executive vice president and provost and is responsible for coordinating IT-related activity across the university, developing collaborations among U.Va.’s academic and administrative units that advance the university’s missions, and working with the university community and its leaders to define and implement a vision for the role of IT at U.Va. Reporting directly to the VP/CIO are:

- The associate vice president and deputy CIO.
- The Advanced Technology Division, which explores emerging technologies and new uses of mature technologies, working in partnership with other units and individuals across the university.
- The Applications and Data Services Division, which supports the instruction, research, and administrative functions of the university by providing applications, performance testing services, and data management and by maintaining institutional databases.
- The Budget and Administration Division, which manages administration, budget and planning, human resources, and purchasing for VP/CIO units.
- The Communications and Systems Division, which is responsible for providing computing and communications services, including computing and network infrastructure, research computing and communications, messaging and voice services, as well as student residential network services.
- The Computing Support Services Division, which provides a wide variety of services that enable computer users to better accomplish their computing goals. Some services are targeted toward specific user populations; others are broad based, serving the needs of many user groups.
- The Integrated System Deployment & Support Department, which is responsible for maintaining and supporting the Integrated System, U.Va.’s financial and human resources ERP system. The university is on schedule to complete the implementation of the student portion of this integrated system by the end of 2009, replacing its homegrown Integrated Student Information System (ISIS).
- The Information Security, Policy, and Records Office (ISPRO), which directs the university’s information security program, formulates and enforces IT policies, advises the university on state governmental IT issues, and is respons-

---

**Managing Sensitive Data at the University of Virginia**

ECAR Case Study 8, 2009
sible for the university’s electronic and physical records management program. Vice President Hilton charged this office with directing the university-wide initiative to improve data management and stewardship.

The Medical Center manages its own IT operations unit; however, Hilton has policy responsibility for the institution as a whole.

Drivers of Change

Several factors facilitated the university’s multi-layered data management program.

The first is VP/CIO Hilton himself and his views on IT leadership. “I think there is a big distinction between being an operational head of the central IT organization and the institution’s VP and CIO,” explained Hilton. “As the latter, I have concerns for things other than central IT operations, one of which is risk management and risk mitigation.”

As a newcomer to the university three years ago, he applied his views when assessing the institution’s IT priorities. The university’s handling of highly sensitive data worried Hilton. He recalled, “With SSN as the primary identifier, the conversations I had with the COO from the day I arrived centered around not whether we would have data exposure, but when.”

And those data exposures did occur, with U.Va. experiencing two notable incidents, one in 2007 and another the following year. The first was a security breach in a computer application that exposed sensitive information of current and former U.Va. faculty members. The next entailed a stolen laptop with the personal information of 7,000 students, faculty, and staff. The incidents created a second facilitating factor—a communal unease with current data handling practices. “The breaches’ associated publicity helped people realize that these are more dangerous times,” explained Valerie Larsen, director of the Center for Instructional Technology. “Many people felt it was time to make some adjustments accordingly.” The first breach hit faculty members particularly hard. “It exposed their personal data, and this brought the problem directly home to them,” added Shirley Payne, assistant VP for Information Security, Policy, and Records.

The third driver was the increasingly decentralized data environment. Fifteen years ago, faculty and staff relied more heavily on central IT to address their institutional data needs, but evolving technology enabled departments and individuals to work directly with institutional data in easier and more sophisticated ways. But again, a sense of unease was percolating. “The chief technology officers in each school understood the situation,” stated Payne. “I have had no pushback from any of them about our data initiatives. As one CTO said, ‘We need to identify this highly toxic data and give it to the central IT organization to manage. After all, the best way to protect the data is not to have it.’”

The regulatory environment also prompted a reassessment of data handling practices. Payne cited the more restricted federal and state data privacy and security environment that has evolved since the 1990s. “It is very clear to us what our most sensitive data are: data that can lead to identity theft and Health Insurance Portability and Accountability Act (HIPAA)—protected data from the U.Va. Medical Center, clinics, and certain other areas of the university.” In addition, the Commonwealth of Virginia passed Virginia Code § 59.1-443.2 in spring 2007, which restricts the use of SSNs except where there is a legal mandate AND essential business practice, and it requires significant institutional commitment to comply. It goes into effect in July 2010.

Hilton, the data breaches, and the changing environment made apparent to U.Va.’s senior administration the need for stronger data stewardship. “From a practical point of view
of protecting the university, I had concluded that I needed to be supportive of good data management practices on behalf of the entire institution,” stated Leonard Sandridge, executive vice president and COO. “We should be very clear that we expect those responsible for a university operation to fall in line accordingly.” This strong senior administration support bolstered Information Technology and Communication’s (ITC’s) activities.

**Previous Endeavors**

U.Va.’s current initiative builds upon two previous actions. Although neither satisfies today’s needs, they both provide groundwork from which the new program is being built.

**Administrative Data Access Policy**

The university’s 1994 policy on administrative data access laid the foundation for today’s work by offering the initial university definitions of data in three categories, then defined as legally sensitive data, limited-access data, and general administrative data. It outlines university employees’ roles and responsibilities for data in several categories, including data stewards, data users, and data sponsors.

The policy delineates other facets of data usage; for example, access, protection, and maintenance of data quality and accurate presentation of data. Although comprehensive when it was introduced, the policy was last revised in 2001, and as Brian Davis, associate director of the Information Security, Policy, and Records Office, stated, “Things like data protection meant one thing in the 1990s when the university first published the Administrative Data Access Policy and mean another thing today. The threats have changed, the risks have changed—what data is available has changed, too.” For more information about the policy, see http://itc.virginia.edu/policy/admindataaccess.html.

**Information Technology Security Risk Management Program**

Another precursor is the university’s Information Technology Security Risk Management (ITS-RM) Program, which requires all university departments to identify sensitive department data and assets, to assess potential threats to those resources, and to determine the appropriate level of security to be implemented to safeguard them. (See http://itc.virginia.edu/security/riskmanagement.)

The program was launched in April 2004, followed by a university policy in November 2004 requiring all departments to participate in the ITS-RM program. All departments were required to complete their risk assessment by July 1, 2007, and to review, reassess, and update their IT risk assessments as needed or at least every three years.

The four-step program process includes

1. *IT business impact analysis*—identification of information, computing hardware and software, and associated personnel that require protection against unavailability, unauthorized access, modification, disclosure, or other security breaches;

2. *IT risk assessment*—determination and evaluation of threats to the resources identified through the business impact analysis;

3. *IT business continuity planning*—development of a plan for restoration of resources identified in the business impact analysis and for interim manual processes to continue critical business functions during the restoration process; and

4. *evaluation and reassessment*—development of a plan to review, reassess, and reimplement the plan on a regular basis.

Upon completion of its report, each department submitted it to the ISPRO for university review and possible remediation.
Although the ISPRO managed the program’s design, training, and compliance, each department completed its own risk assessment because of its familiarity with its mission and the IT assets required to fulfill that mission. The department managers could subsequently use this knowledge to prioritize and restore their assets following a disaster. The ISPRO, working with other areas (for example, auditing), distributed to departments a program packet consisting of instructions, templates, and general information about risk management and common risks.

The ITS-RM program performed two important functions to facilitate future initiatives:

- It created for departments a baseline of information (for example, stores of sensitive data) and a process to be used to comply with future data requirements.
- It spurred further data management efforts because an inventory of all the servers containing legally protected data now existed. “I had some misgivings because although I wanted the inventory, at that point in time we had no approved plan or resources to remediate this,” stated Payne. “It was a powder keg. From a due diligence standpoint the urgent need to better secure this sensitive information was crystal clear.”

**Multi-Layered Strategy**

Data stewardship is driven by security, privacy, and data retention requirements, as well as data access approvals and procedures, and with the support of senior administration the ISPRO embarked on its initiative in 2007 to tackle these issues.

Given the university’s past operational and archival history, fulfilling this undertaking was a complex task. So ISPRO’s strategy was to tackle the problem in discrete chunks of the institution’s data flow—in other words, to clean the stream of institutional data going forward and then to remediate past records and protect what could not be remediated.

This strategy aims to limit highly sensitive data by cutting off its distribution or substituting non-essential highly sensitive data in various university forms and processes. It also aims to eliminate as much as possible all instances of non-essential highly sensitive data in archival department paper and electronic files.

Both actions decrease risk over time. As Davis explained, “We knew that all incidences of highly sensitive data would not be eliminated during the first round. The goal is to get everybody to do as much as they can, which gets rid of the easy 80%. The next year, we will get rid of the next easiest 80%, and so on. We will reduce risk every year, making the number of incidents smaller and smaller as time goes on.” Figure 1 illustrates the multi-layered security strategies used, which this section details.

**Hardening and Securing the IT Infrastructure**

Firm IT security, ensuring that data resides in a protected and fail-safe IT infrastructure that precludes loss from criminal acts or environmental events, is a precondition of good data management. And in 2007, Hilton felt that U.Va.’s IT infrastructure was not quite up to this task. Some of the servers and mainframes were aging, and disaster recovery and business continuity plans needed to be enhanced to minimize risk. Without such changes, the other initiatives would have rested on an unstable foundation. As Hilton explained, “The project is not framed in terms of just data remediation, but how we protect the data by bolstering the redundancy and resistance to threats of U.Va.’s IT infrastructure.”

The Hardening and Securing of Infrastructure project addresses this goal. Begun in 2007, this multiyear project works to eliminate single points of failure in mission-critical university systems and services. Some
Using this approach, U.Va. created a three-tier data classification that updated the classifications in the university’s 1994 Administrative Data Access Policy. In the updated classification,

- highly sensitive data is defined as personal information that can lead to identity theft if exposed (that is, Social Security numbers, passport numbers, driver’s license numbers, financial account numbers) and health information that reveals an individual’s health condition and/or history of health services use (that is, HIPAA-protected information);
- nonsensitive data is publicly released information; and
- moderately sensitive data is the default classification for data that falls between the other two categories.

The ISPRO worked with the president, the executive vice president and COO, the executive vice president and provost, and the vice president and CIO to delineate U.Va.’s most sensitive data. They defined the new classifications, guided by relevant Commonwealth of Virginia laws (for example, any data that could lead to identity theft) as well as HIPAA specifications.

The first university policy to follow this data categorization is the policy on Electronic Storage of Highly Sensitive Data approved in
June 2008 to limit the circumstances for the storage of highly sensitive data on university and personally owned mobile devices, media, laptops, and desktop computers, with the goal of avoiding the unauthorized exposure of highly sensitive data. The policy specifies the security requirements under which this data may be stored. (See http://itc.virginia.edu/security/highlysensitivedata.)

The policy mandated a two-phase approach to compliance. Phase 1 required immediate compliance for laptops, mobile devices, and mobile media like flash drives because of their higher risk of theft or loss. All university personnel had to scan these devices for highly sensitive data. The users were required to delete or move to a secure server any highly sensitive data not needed for an approved business purpose or record retention. If the highly sensitive data needed to remain on the device, the user had to submit a form to the department head or chair for review and subsequent written approval by the responsible vice president or dean.

Phase 2 applied to desktop computers and could be completed along with the Social Security Number Initiative described in the next section. In July 2008, all departments submitted reports to the ISPRO that listed any highly sensitive data on individual desktop computers, which Payne’s area pulled together into a summary report for senior administration review. The vice presidents had to endorse any submitted requests to continue to use highly sensitive data in their areas. In July 2009, all departments had to confirm with Payne’s office their completion of any remediation plans.

**Social Security Number Initiative**

A parallel initiative phased out the systematic use of SSNs in university business and academic processes. (See http://www.virginia.edu/ssninitiative.) As noted, the SSN was the university’s personal identifier, and therefore universal, as people used SSNs to match people from different university offices, to transact businesses and processes (for example, to process financial aid forms), and to track forms and processes. As Davis described, “SSNs were deeply entrenched, and we needed to identify and eliminate the tentacles of SSN usage. Departments asked for SSNs, frequently not because it was required, but it was convenient. People got in the habit of asking for it. Staff members received permission to use SSNs for one purpose and then created a departmental system that takes advantage of them. So permission was given for one use, and people were still using SSNs three or four steps down the process because people were passing them from one to another and using them for a completely different and undocumented purpose.”

To augment the SSN initiative, in December 2007 U.Va. passed an institutional policy, Protection and Use of Social Security Numbers, that formally classifies SSNs as highly sensitive data and authorizes SSN use only where there is no feasible or legal alternative. The continued use of SSNs required the approval of the SSN remediation team and appropriate university officials. The policy decrees that no new system can use an SSN as the primary identifier; specifies conditions under which SSNs may be collected, used, or reported; and ensures access by only the appropriate departments and staff members within those departments. In addition, it requires an inventory of the records that contain SSNs; secure access and storage of approved records with SSNs; and secure disposal of noncomplying records that contain SSNs. (See https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-014.)

All new records had to comply immediately with the policy, and departments adopted a phased compliance for existing records and systems. All departments had to identify where their information systems solicited, collected, or stored SSNs electronically or on paper and had to state where SSNs were:
Managing Sensitive Data at the University of Virginia

ECAR Case Study 8, 2009

- used as an account number or identifier;
- used in interactions with other university systems or with external third parties;
- archived in paper or electronic records;
- displayed on documents or screens;
- transmitted electronically, online, via mail or fax; and/or
- stored in a document imaging system.

By July 2008, all units had to submit to ISPRO an inventory of all records and information systems that used SSNs and develop an approved remediation plan for non-essential SSN usage. All remediation plans had to be enacted by July 2009. If approved, SSN records had to be stored on highly secured computer equipment or in locked file cabinets.

**University ID/ID Card Project**

If U.Va. was to restrict the use of SSNs, the question became what to use as a substitute. Coincidentally, Virginia Code § 59.1-443.2 on SSN usage now required the removal of SSNs from all identity badges. So U.Va. had to reissue its ID badges because they contained a person’s photo and the SSN embedded in the magnetic strip on the back. In addition, a growing security risk was ID card–dependent systems that might store and/or transmit SSNs.

Again, the executive vice president and COO, the executive vice president and provost, the vice president and CIO, and other university stakeholders were engaged in identifying an alternative. They decided to create a new nine-digit university ID number that stays with a person for life—whether student, university or Medical Center employee, or alumna/alumnus. This university ID would be incorporated into all ERP systems, enabling disparate systems to interact without falling back on SSNs. The new nine-digit design facilitated the assignment of new university ID numbers, the creation of solutions to convert SSNs to the university ID numbers in electronic files, and the improvisation of interim solutions. For example, the library designed a feature for its checkout desktops that displays a person’s university ID number, even if the person input his or her SSN.

**Project Implementation**

The similarities between the sensitive-data-handling and SSN initiatives enable the ISPRO to coordinate both projects in tandem, which this section details.

Since these initiatives cut across all university business and academic departments, a broad constituency of project members was needed to guide the projects. For example, the SSN initiative’s core team consists of 23 members from university academic, business, and Medical Center areas. “Everyone knew the officially documented incidences of SSNs, but this group could identify shadow uses,” stated Davis. “They could piggyback off of each other’s knowledge to identify how data feeds into and out of the university as well as between schools and areas. Everyone had a partial snapshot, and getting them to overlap was difficult. SSNs were so embedded into the system, people did not know all the areas of use.”

**Confidential Data Handling Blueprint**

One tool that Shirley Payne, assistant VP for Information Security, Policy, and Records, relied upon during U.Va.’s multiple projects was the Confidential Data Handling Blueprint, a toolkit compiled (and refreshed in spring 2009) by the EDUCAUSE/Internet2 Higher Education Information Security Council (formerly the Security Task Force). It provides a seven-step guide and links to relevant higher education, government, and industry online resources. “It looks at the whole spectrum of the process,” stated Payne. “I used it to recommend courses of action to our senior administration and to demonstrate our progress.” For more information, see https://wiki.internet2.edu/confluence/display/itsg2/Confidential+Data+Handling+Blueprint.
One of the first actions performed by the ISPRO was creation of a formal communications campaign. Payne and Davis visited university departments and worked with the Office of Public Affairs to create an awareness campaign around campus.

Next and most importantly, the office created tools to help departments with their compliance activities. “It wasn’t that we just delivered the policy, we give them the tools to instruct faculty and staff about compliance and implementation,” stated Payne. The office used the same methodology as the ITS-RM program, distributing a set of templates for individuals and departments to inventory incidences of SSN/highly sensitive data usage and to identify the situations in which they are used. The tools were designed for departments not only to eradicate non-essential instances of SSNs and other highly sensitive data but also to redesign processes to accommodate the new guidelines. The following templates are available for review at http://www.virginia.edu/ssninitiative/policies.html#forms:

- The SSN Inventory Worksheet walks the department through various scenarios to collect information from faculty and staff regarding where SSNs are collected and stored.
- The SSN/Credit Card Data Machine Scanning Tracking Sheet tracks the individual machines that scan SSN information.
- The Tracking Sheet for Identified SSN Usage asks the department to list the processes and systems of SSN usage, the person responsible for them, and whether the department plans to eliminate or continue their use. If the department plans to continue usage, it has to fill out a request form to receive vice president or dean approval to do so.
- The Tracking Sheet for Credit Card Information and Protected Health Information Data requests similar information as the SSN tracking sheet in the previous entry.
- The SSN Remediation Plan asks the department to list instances where SSNs are to be eliminated and provides plans for remediation.

The Office of Public Affairs provided other tools, most notably purchasing a site license for Velosecure’s Identity Finder software so that departments and individuals could scan laptops, desktops, servers, and media for SSNs, credit card information, and other highly sensitive data. U.Va. customized Identity Finder to scan for medical records. Identity Finder enabled departments to keep an accurate inventory of all highly sensitive data stored. Another tool was an interface developed by the Communications and Systems Division to allow a one-time conversion of SSNs to equivalent university ID numbers.

The University Records Management Office assisted in these projects by providing advice and guidelines on which records containing highly sensitive institutional data to retain, how to store them securely, and how to dispose of out-of-date records. With these new guidelines, departments and areas could purge their outdated electronic files as well as tons of hard copy records. To facilitate this process, the University Records Management Office sponsored a records collection day during which departments could destroy their records in a university-hired shredder truck. An estimated 11 tons of records were shredded that day.

Serendipitously, U.Va. instituted its policy on SSN use in December 2007, and the Virginia Code § 59.1-443.2 on SSN use passed the following spring. Similar to U.Va.’s SSN project, the statute required by October 2008 all state agencies, including U.Va., to inventory and explain all incidences of SSN use, to point to a state or federal statute that required the SSN use, and to verify that its collection is essential to the agency’s/institution’s business. The state law further required remediation of noncom-
compliant practices by July 2009, a deadline legislators subsequently extended to July 2010. Payne admitted that without the university projects already under way, it would have been difficult to meet the state deadline.

The User Viewpoint

Central data management efforts would have been ineffective without the involvement of university departments. Staff members carried out these projects, which in many cases altered their work activities. Therefore, to gain a complete perspective, one must ascertain the user’s point of view. The four department snapshots reviewed in this section offer a better understanding about the user’s implementation experience and the subsequent operational implications.

The College and Graduate School of Arts and Sciences: How to Accomplish Remediation in a Large College

Each university area had to comply with the ISPRO’s data security and handling initiatives, but few areas are as complex as the College and Graduate School of Arts and Sciences (A&S). U.Va.’s largest college, A&S comprises 27 academic departments and 50 centers, institutes, and units. Nancy Bertram, associate dean for Management and Budget, served as the administrative leader responsible for the area’s compliance with the sensitive-data-handling and SSN initiatives. Valerie Larsen, director of the A&S Center for Instructional Technology, and Robert Campbell, director of A&S Computer Support, were the project managers, assisting areas directly with their compliance efforts.

To facilitate departmental support, Bertram required a joint faculty and administrative team from each academic department to be responsible for the project. As a first step, Larsen and Campbell held a series of workshops for the area teams to educate them about the project requirements and the available tools to assist them. They created a course site on Collab, the U.Va. courseware system, to function as the college’s primary information and communications site for the project. Larsen and Campbell met face to face with representatives from numerous areas to answer questions and assist with planning.

Before rolling out the tools created by the ISPRO to the entire college, Larsen coordinated pilot projects in four A&S areas—including her own—to refine the remediation process. Larsen’s area filled out the templates provided by the ISPRO first, and then the other pilot areas completed theirs, building upon Larsen’s area’s initial work. The result was a largely completed template that other A&S areas could then adapt. “Because many of our department forms are similar, the vast majority of A&S areas opted to use the nearly completed template to account for their specific incidences of SSNs and other highly sensitive data,” explained Larsen. “This reduced each area’s completion time by permitting units to focus their energy on the identification of specific instances, remediation planning, and implementation. While an enormous amount of effort within units was devoted to identification, planning, and remediation, the template facilitated the process by making it easier to get started, identify targets for remediation, encourage common reporting mechanisms, and foster communication.”

A&S’s Local Support Partners (LSPs are departmental technical support personnel) could help staff members download the Identity Finder software, scan reports, and answer questions, but they were not permitted to analyze reports or make decisions about the content within the report on people’s computers. This minimized risk and reinforced each individual’s responsibility for his or her data.

A&S areas submitted their initial reports for the university’s July 2008 deadline. In addition, A&S areas were required to submit
Managing Sensitive Data at the University of Virginia

ECAR Case Study 8, 2009

an interim report about their remediation progress in January 2009 to keep them focused on the project. All but one area met the 2009 deadlines for SSN remediation reports. Although A&S units complied with the deadline, their reports are still in review and modifications may yet be required.

The sensitive-data-handling and SSN initiatives have impacted A&S in different ways. Some departments streamlined their records archives, in some cases destroying decades’ worth of outdated paper files. Many faculty members were surprised by the amount of highly sensitive data that Identity Finder located on their computers. Larsen stated that far less highly sensitive data is now stored locally at A&S departments. For example, the Office of the Dean used to keep copies of a new hire’s personal identification, but everything is now forwarded to the official office of record, University Human Resources.

Student System Project: Adaptation during Implementation

As Susan Barr, director of the Student System Project (SSP), stated, “It is easier to implement changes in a new system than to retrofit an old system.” Barr speaks from experience, for as the university implemented its sensitive-data-handling and SSN initiatives, her area was implementing a new PeopleSoft student ERP system to replace U.Va.’s ISIS home-grown system. The project, which reports to the executive vice president and provost, began in fall 2004 and is scheduled for completion in December 2009. System modules include Academic Advisement, Campus Community, Campus Self Service, Enterprise Gradebook, Enterprise PeopleTools, Enterprise Portal, Financial Aid, Recruiting and Admissions, Student Financials, and Student Records. The Student ERP system is the third phase of the university’s Integrated System project, with Finance and Human Resources implemented in 2001 and 2002, respectively.

The Student System Project is on time and on budget, but Barr conceded that “the group has had to adapt very quickly as new data infrastructure and policy changes have come up.” When the project began in late 2004, U.Va.’s emphasis on data security had not commenced. “The parallel evolution is a challenge because at the same time we are implementing the software, the university is codifying its data handling and data security processes. As it turns out, many of the changes made to secure data are reflected in the student information system for the first time.”

According to Payne, “The student system implementation project team has done a fantastic job in engaging many people across the university in helping to raise awareness of data protection.” As Student System Project director, Barr was plugged into the sensitive-data-handling and SSN initiatives very early. She is a member of the SSN Initiative Core Team and vetted early versions of the new sensitive-data-handling policies with the Student System Project’s extensive governance structures. “I did my best to inform all these groups about that work because while some of it was posted, some of it was not.” Barr used the project member database of more than 600 people to communicate updates.

Barr worked closely with central IT to foster understanding. Early in the project, representatives from central IT divisions, the Student System Project, and the Integrated Student Information System (ISIS) created a memorandum of understanding about the project’s technology requirements. Payne has met periodically with Student System groups to update and explain new data security and handling policies. A group called the Issues of Common Interest emerged that brought together Barr, Payne, the director of the Communications and Systems Division (who is also codirector of the Hardening and Securing of Infrastructure
project), representatives from the Integrated System Deployment & Support Department and ISIS, and others to address topics of mutual concern.

From an implementation perspective, Barr’s group worked closely with the ISPRO as well as the Hardening and Securing of Infrastructure project group to incorporate their activities into the new student information system design, for the groups’ activities at times have added further complexity to an already complicated project.

A good example is the design of U.Va.’s three application processes for undergraduate students, graduate students, and visiting students (defined as non-degree-seeking students attending U.Va. for a short time or continuing education students). Within each application process, different scenarios affect whether a student provides an SSN. For example, undergraduate admissions uses the Common Application, a national application nonprofit service used by more than 300 colleges and universities, which requests the applicant’s SSN as an option; graduate schools rely on Hobson’s recruitment and application tools, wherein SSNs are optional, too. Under federal law, a request for financial aid, however, mandates that the applicant supply an SSN, since the federal application for student financial aid also requires this information. The visiting student application does not even request an SSN because the current application process is unsecured, requiring the applicant to fill out a web-based PDF form and submit via mail or fax. (Development work began in fall 2009 to create a secure web application that feeds into the main student information system.) A decision on a unified approach governing the use of SSNs in applications for admission is still pending because the university is waiting to see if the Commonwealth of Virginia will include the prohibition of SSN collection in its legislative directives in the future.

Departmental access to data became an issue, since some schools, departments, and units had systems that plugged into the historical Information Warehouse (U.Va.’s data warehouse that stored all student information prior to fall 2009) for data transfer into local systems. Now all information is stored in the student information system and the reporting environment, both of which operate in a secured network environment. The sensitive-data-handling and SSN initiatives identified data access points to each of these systems and thereby enabled central IT to inspect appropriate administrative and academic areas to ensure their systems are secure enough to plug into the new student information system.

Finance and University Comptroller: Changes Ripple through Current Processes

The Division of Finance and University Comptroller comprises Accounting Services, Financial Reporting & Analysis, and Student Financial Services. These areas routinely handle highly sensitive data. For example, Student Financial Services is allowed to capture SSN information to process student financial aid requests to the federal government. Although the Student System Project could incorporate new policies and procedures into a new system, Steve Kimata, assistant vice president for finance and university comptroller, faced the prospect of modifying his area’s current business practices and processes to accommodate the sensitive-data-handling and SSN initiatives. One immediate benefit is that it did help his area to prepare for the new student information system implementation.

As noted, the ISPRO provides tools for departments to identify and remediate their sensitive data and SSN handling. “We made it very clear from the beginning that this was a business process issue, not a technology issue,” stated Davis. “Areas may rely on their technical personnel for
support and advice to improve data security, but the technical personnel cannot identify the required data for business personnel to complete their jobs.”

As Kimata noted, “The SSN initiative and other new policies had some very practical applications for us in a number of different dimensions.” Internally, numerous reports had to be reprogrammed. For example, a financial aid report, created more than 20 years ago in the old ISIS student information system, identifies who received financial aid and the subsequent charges for each department—and contains SSNs. The department had to reprogram this report and others to eliminate the SSNs. Old paper-based reports and electronic files had to be destroyed in accordance with data handling and university records management policies to avoid inadvertent information disclosures.

Interdepartmental processes were impacted, too. Reports with highly sensitive data could no longer be e-mailed, forcing U.Va. departments to pick up their reports in person. Since financial services collects overdue accounts for the entire university, including the Medical Center, HIPAA issues came into play. This caused Kimata to work with the Medical Center to determine how his area could use their data in a compliant manner.

External transactions with vendors and government agencies were also affected. In a push for greater transparency, the Commonwealth of Virginia required the collection of information about state expenditures, which is subsequently displayed on a state website. Kimata had to consult with the commonwealth so as not to share highly sensitive data when complying. Some small vendors who used their SSNs as their corporate ID numbers had to obtain Employer Identification Numbers from the federal government.

The complications of new procedures extend to customers of the division’s offices. Student Financial Services could no longer accept fax transmissions and e-mail messages containing SSNs. “Students did not think anything about faxing or e-mailing us their Social Security number,” stated Kimata. In response, Kimata’s area launched an awareness campaign to educate students and other departments about the new policies regarding SSN transmission.

Laptops, PCs, and mobile devices were scanned using Identity Finder to find and eradicate all inappropriate uses of SSNs and highly sensitive data that had accumulated in these devices over the years. Kimata plans to continue scanning department devices on an ongoing basis, though he claimed, “It’s not nearly as problematic anymore because we don’t get many files that contain SSNs. We just want to be careful.” Individuals who were approved to store highly sensitive information on their mobile devices had to password-protect and encrypt them. Flash drives could no longer be used to store highly sensitive information.

When reflecting upon his area’s experiences, Kimata commented, “It was a lot of work in a short period of time, but everybody agrees it was necessary and it was something that we all had to deal with. Stepping back, it caused us to look at things differently because we are entrusted with our customers’ data and we have to take care of it properly.” Kimata concedes that the initiatives slowed down his area’s operations at times and may have temporarily reduced efficiency. “But once we explained the situation in terms of protecting their personal data, customers became understanding about the situation,” continued Kimata. “We compare it to going through the airport security check-in.”

The work is ongoing, as the area still encounters new incidents of handling highly sensitive information. Just before this case study visit, a new situation arose without an obvious resolution, which Kimata, Payne, and other relevant parties will address. “We are still grappling with it,” conceded Kimata. “It is an ongoing effort.”
Medical Center: The Added Dimension of Patient Data

At U.Va., the university and the Medical Center report to the same Board of Visitors; as vice president and CIO, James Hilton leads IT policy for the entire university, and thus all the data management activities described earlier apply to the Medical Center as well, with the extra privacy and security issues that medical data entails.

The Medical Center’s handling of health-related information provided the center with a head start on the university’s emerging sensitive-data management activities. “It was an easier onion to peel because people understood the data access concept of ‘need to know’ from dealing with HIPAA compliance,” stated Wayne Martin, Medical Center information security manager. “So the university data management initiatives moved forward fairly easily and fairly rapidly.”

But the Medical Center works with SSNs and sensitive information of two sorts. The first falls under the university’s sensitive-data-handling and SSN initiatives for student, faculty, and staff personal data; the second type, patient information, is a harder nut to crack. The Medical Center deals with many government agencies and finance companies, most of which require SSN information. And an SSN is the single identifier that follows a person throughout her or his life, regardless of name, address, or insurance coverage changes. “The question becomes how to send data in spreadsheets, Word files, and databases that is intimately linked to a patient’s account,” explained Martin. He conceded compliance in the patient area is a far more challenging proposition. One means to address this is to move the SSN lower in the patient’s list of personal identifiers. Rather than asking for an SSN first, Medical Center employees try to verify name, address, phone number, and date of birth to positively identify a patient before asking for an SSN.

U.Va.’s Next Steps

Data management initiatives are far from complete at U.Va. This section highlights new standards, policies, and activities.

Institutional Data Protection Standards

U.Va. released new Institutional Data Protection Standards in August 2009 that build upon its Electronic Storage of Highly Sensitive Data Policy as well as the Protection and Use of Social Security Numbers Policy. The new standards formalize activities from the sensitive-data-handling and SSN initiatives. (See http://www.itc.virginia.edu/security/dataprotection.) “This is the first central standard that we have issued that states very specifically the minimums for data protection at the university,” stated Payne. The standards outline the handling and protecting of highly sensitive, moderately sensitive, and not sensitive university administrative, academic, and research data by several dimensions:

- **Responsibility for data:** The policy spells out data accountability, naming vice presidents and deans as the university officials with the responsibility for determining who has access to highly sensitive data and for appointing individuals with responsibility for ensuring the protection of highly sensitive data. The policy requires vice president/dean approval for a person to store highly sensitive data on his or her individual-use computing device, smartphone, and electronic media. Interestingly, when Payne originally wrote the policy, she specified sign-off at the department head level, but senior administration feedback made it a vice president/dean–level responsibility.

- **Data transmission:** Highly sensitive data may not be communicated via e-mail, with the exception of the Medical Center because it has a very strong business need to send e-mails
that might contain HIPAA data and has developed a secure transmission means. For moderately sensitive data, the policy states that e-mail transmission is not recommended. For nonsensitive data, the policy states that transmission medium is not an issue.

- **Data storage and destruction:** If a server stores highly sensitive data, it has to be behind U.Va.’s highest-security firewall environment and housed in a highly secured location; users accessing these systems do so through mandatory two-factor authentication. Assurance that the storage device is going to be scanned on a regular basis is needed. A department that is storing highly sensitive information will need to conduct a risk assessment and an annual refresh of its disaster recovery plan and will be subjected to more frequent audits. The policy requires that all data no longer needed be securely destroyed, that is, in a manner that makes subsequent exposure impossible.

**Forthcoming Data Classification Policy**

The Institutional Data Protection Standards Policy is a predecessor to a forthcoming university policy to codify data classification. Although still under development, the policy will officially redefine the university data categories, define how data classifications are determined (for example, legal regulations and data steward input), and require all university data to be classified, since data classification determines security and accessibility as defined by the Institutional Data Protection Standards.

**Formalizing Data Stewardship**

The university’s 1994 policy on administrative data access began the university’s data stewardship initiative. A forthcoming policy on data stewardship builds upon the 1994 policy to describe the university’s philosophy about data management and access as well as to define data stewards, data management roles, and data use responsibilities.

A companion piece to the data stewardship policy is an updated list of university data stewards. The 1994 policy defined data stewards, but over the years the players have changed, and the issue of stewardship is now more distributed. For example, Barr and others in the Student System Project created an expansive data stewardship structure that maps to the new student information system. They worked with stakeholders to identify data stewards in the context of the university’s policies and standards. For example, new data stewards were assigned to represent undergraduate and graduate admissions and undergraduate and graduate financial aid, since each school’s graduate program has its own graduate admissions and financial aid processes. “I had to expand my thinking on this particular issue,” Payne explained. “In the early ’90s, the heads of the undergraduate admissions and financial aid offices were the appointed data stewards for the admissions and financial aid data domains. The implementation of modern ERP applications, however, has enabled more distributed management of subsets of these domains. The appointment of admissions and financial aid data stewards for every graduate school makes perfect sense today,” stated Payne. “There may be similar issues with finance and HR systems, too.” Now Payne is working in consultation with various stakeholders to design a new data steward structure and accompanying processes in these areas as well. Along with this effort, the 1994 policy is being updated to reflect today’s data stewardship responsibilities.

The Medical Center is in the process of formalizing its data stewardship structure.
“We might know culturally and internally who the data owners and the data stewards are, but we are quantifying it now,” stated Martin. “We’re creating definitions, a data steward council and steering committee so it becomes clear to the organization as to who are the data stewards and the data owners.”

**Surpassing State SSN Standards**

As the Commonwealth of Virginia continues its focus on state agencies’ collection, access, and storage of SSNs, U.Va. has decided to proactively tighten its SSN handling policies. The current phase calls for the university not to collect SSNs for university purposes, but only to solicit SSNs when the institution acts as a “pass-through” for an agency—for example, for financial aid processing. “That is a huge switch to see an institution move from a totally reactive position to now proactively eliminating SSN usage, even in areas that state law currently allows,” said Payne.

**Lessons Learned**

Case study participants shared several lessons about their experiences with the data stewardship program, as described in this section.

*Senior administrative support is critical.*

Compared with many IT projects, U.Va.’s data initiatives require extensive—and potentially intrusive—local involvement to address an issue that a department may or may not deem problematic. These characteristics make senior administration support especially critical for the project’s success. This top-level support was very apparent at U.Va. As Executive VP and COO Sandridge stated, “If I think back about some of the challenges, I think it was fair to say that we needed to demonstrate to Shirley [Payne] and her team that we support their professional judgment when they surveyed the situation or made recommendations.”

**It’s no one’s fault.**

When approaching departments about the sensitive-data-handling and SSN initiatives, Payne and Davis made it a point not to place blame on anyone for the proliferation of highly sensitive data. “We told people over and over again that it was not their fault; the university’s practices forced this on you,” stated Davis. The ISPRO positioned the project as an opportunity to rehabilitate university practices to enhance everyone’s personal security, a strategy validated by U.Va.’s security breaches. As Larsen stated, “We approached it from the point of view of making things better. Times have changed and we have to work together to resolve it.” This strategy fostered a more cooperative attitude.

*Set realistic expectations.*

Payne and Davis recognized the enormity of the tasks for departments to update their sensitive-data-handling and SSN processes. Rather than sugarcoat the projects, they made a concerted effort to be up-front and to set appropriate expectations. “We tried to communicate the projects’ potential disruptions and how our office would try to minimize pain,” stated Davis. This honesty helped departments make appropriate preparations for the upcoming projects.

*Plan and execute for the long term.*

COO Sandridge characterized the sensitive-data-handling and SSN programs as “marathons, not sprints. We do not want to be a flash in the pan. We want to be consistent across the board.” Cultural shifts contribute to the projects’ long-term nature. For example, at the U.Va. Medical Center, Martin observed, “I don’t think there can be a project deadline or timeline because we are changing how physicians practice. They are so used to reviewing Patient A’s entire medical record when they need only one or two pieces of information. They have to
change their mind-set from asking for the whole medical record to asking for essential information.” This is a shift that does not typically occur overnight.

**Maintain a strong project core.**

Like other research universities, U.Va. is an assembly of schools and colleges, institutes, the Medical Center, and other organizations. “Being so decentralized, it is hard to get everyone going in the same direction and on board,” stated Kimata. “The more you can convey a well-coordinated, central focus and an overall institutional mandate, the better off you will be. If you don’t, some people will not get the message or hear it as a priority. If it is too vague, it is hard to get everyone moving.” For that reason, the ISPRO released specific university policies that define steps and deadlines for compliance.

**Create early engagement with stakeholders.**

As Barr stated, “How things look from the outside is not the same as they look from within central IT.” Because the “outside” represents a vital project component, it was important to engage stakeholders in a structured manner from the onset to solicit their input and buy-in on project decisions, strategies, and actions. It keeps them up to date about progress, best practices, and bumps in the road as well as facilitating a supportive attitude throughout the project’s duration. From their local standpoints, the stakeholders provide fresh perspectives and feedback to central IT.

**Strong communication and governance provide user guidance and structure.**

Numerous commentators at U.Va. emphasized the criticality of communication within and across units of all sizes and the importance of governance to support and oversee significant changes. However, almost as often, they mentioned that any new initiative would need better ongoing emphasis on communication and better governance structures.

**Facilitate compliance by providing tools and detailed procedures.**

The ISPRO tried to facilitate compliance by “doing as much up-front work as possible,” stated Larsen. She pointed to the available templates that walked departments through the process of identifying incidences and uses of highly sensitive data and SSNs. Larsen took this a step further by entering common incidences of highly sensitive data in the template to facilitate other A&S areas’ completion. “We set it up so areas had to conduct the least amount of research to comply,” stated Larsen.

**Saying “no” is critical.**

Hilton argued that saying “no” supported his effort to transform central IT from an organization that strove to help everyone to one that deals with sourcing and delivering enterprise tools. The multi-layered initiative has focused central IT’s functions to everyone’s benefit.

**Conclusion**

As data continues to proliferate and security risks continue to accelerate, creating a sound and safe environment in which to handle and store data is an imperative, but difficult, task. Yet during these past three years, U.Va. has worked to create a data environment that proactively anticipates future requirements. VP/CIO Hilton’s vision, the ISPRO’s project management and outreach, and most importantly the institutional buy-in and sacrifices all contributed to this change. The result is heightened data stewardship in which university members more fully understand the necessity of creating and complying with solid data management policies to protect an important university asset—its institutional data.
Endnotes
2. Ibid., p. 76.
4. Ibid.

Citation for This Work