AMERICAN BAR ASSOCIATION

JUDICIAL DIVISION

SECTION OF SCIENCE AND TECHNOLOGY LAW

TORT TRIAL AND INSURANCE PRACTICE SECTION

REPORT TO THE HOUSE OF DELEGATES

RECOMMENDATION

RESOLVED, That the American Bar Association adopts the black letter of Sections 1.60 through 1.64 Relating to Court System Automation to amend the Standards Relating to Court Organization and replace current Sections 1.60 through 1.64.

FURTHER RESOLVED, That the American Bar Association adopts the black letter of Section 2.80 Relating to Trial Court Responsibilities for Court Automation to amend the Standards Relating to Trial Courts to replace current Sections 2.80 through 2.83.

Black Letter of Revised Sections 1.60 through 1.64

1.60 Statewide automation structure

Regardless of a state judiciary's organizational structure, many functions must be performed at the state level by the administrative office of the courts under the supervision of the Supreme Court, with an appropriate governance mechanism, for all levels of courts. The functions include court automation strategic planning, standards and policy setting, infrastructure development, deployment and maintenance, procurement and operation of basic statewide capabilities.

a. Governance mechanism

The Supreme Court, by administrative order, should establish a governance body composed of representatives of all levels of courts within the state, including judges, administrators and technology specialists, and representatives of the bar and executive branch agencies with whom the judiciary regularly exchanges information. The role of the governance body should consist of policy and priority setting, strategic planning, ensuring compliance with national standards, setting state standards, and monitoring the progress of statewide court automation.

b. Statewide automation functions

Certain automated applications should be established and operated by the administrative office of the courts on behalf of all courts within the state.

The necessary applications at the state level include:

i. A common means for communicating with the courts and providing access to statewide court information

ii. Statewide data repository

iii. Statewide telecommunications and training network

iv. Statewide maintenance and support

c. Statewide architectural and strategic planning

d. Statewide data standards

e. Statewide administrative policies

f. Statewide procurement and licensing

g. Statewide support for business process redesign

1.61 Comprehensive court automation applications

The state should ensure that all courts have a core set of automated applications.

a. A case management information system having at a minimum the functionality set forth in the Conference of State Court Administrators/National Association for Court Management functional standards.

b. Standard office automation applications appropriate for each person's duties, including PC or server hosted fax processing, word processing, email, Internet access, spreadsheet, super user data base applications, ad hoc reporting packages, calendar, financial processing, graphics, and project management software.

c. Applications to support an electronic document management environment, including electronic filing, electronic service, electronic access to court documents, automated workflow management, and document and file retention and storage.

d. Standard courtroom technology, including audio amplification and recording, video recording, video and telephone conferencing, evidence presentation equipment, and display monitors and screens for the judge, courtroom personnel, attorneys and parties, jurors, witnesses, and spectators.

e. Statewide and local court websites, including information about the court system, information about the court's rules and processes, access to statutes and court precedents, fillable forms, access to public data in the repository, instructions for persons representing themselves, electronic filing and payment process, calendar access, and court performance and workload data.

f. Access to automated legal research

g. A jury management application

h. Automated applications for recording and maintaining the court record

i. Administrative applications

j. Applications to support ancillary court services

1.62 Information sharing with other justice entities

Courts should obtain as much information as possible in electronic form from executive branch agencies and lawyers and provide as much information as possible to them in electronic form, following accepted industry standards.

1.63 Development and support of automated applications

In developing new automated applications, courts should follow these best practices:

> **a. Courts should insist that their applications comply with nationally applicable standards**
>
> **b. Courts should take advantage of open source and public domain software when possible and practical**
>
> **c. Courts should exhaust all possibilities for using or adapting public domain, open source, or commercial software products before deciding to build their own software applications**
>
> **d. Courts should require software vendors and court staff to use a "spiral" development process in producing and enhancing new applications**

1.64 Security

Courts should employ sufficient architecture, applications, and procedures to minimize recognized threats to the security and integrity of court data, documents, and processes.

2.80 Trial court responsibilities for court automation

The trial court is responsible for day to day operation and maintenance of all of its automated applications. To the extent that the court operates hardware and software different from that supported by the administrative office of the courts, the court is responsible for support of that equipment and software.

Black Letter and Commentary of Revised Sections 1.60 through 1.64

Commentary on Sections 1.60 through 1.64

Introduction to the 2005 revision of the standards relating to court automation

Standards 1.60 through 1.64 were adopted by the American Bar Association in 1990. They are fifteen years old. When they were developed, the drafters consciously attempted to create principles that were sufficiently global and general that they would not rapidly become obsolete. They were written to be broad enough to encompass changes in specific technologies and to set forth only the way in which courts should go about making decisions about court technology. Despite the vision and forethought of the drafters, the current standards could not take into account the major shifts in technology that we have all seen. They are now completely out of date and largely inappropriate to today's technology decisions.

The 2005 revision has been prepared with this experience in mind. The drafters of this revision are under no illusion that this work will have more durability than that of the 1990 drafters. The pace of change in technology continues to be astonishing. This revision makes no claim that the concepts presented will be any more enduring than the 1990 version of court automation principles. The drafters, therefore, have attempted merely to set forth the "best practices" and ideas as we understand them in 2005.

The only way in which these standards can be of continuing value is for the American Bar Association to revisit and revise them no less frequently than every three years. The maintenance of obsolete standards – in this and in any other area – is likely to cause more harm than good. Consequently, in putting these revised standards forward for adoption by the Association, the Judicial Division recommends that the Association revisit this topic no later than the beginning of 2008. In the meantime, all readers of these standards should be alert to the emergence of new technologies and of new national standards for applying them.

1.60 Statewide automation structure

Regardless of a state judiciary's organizational structure, many functions must be performed at the state level by the administrative office of the courts under the supervision of the Supreme Court, with an appropriate governance mechanism, for all levels of courts. The functions include court automation strategic planning, standards and policy setting, infrastructure development, deployment and maintenance, and procurement and operation of basic statewide capabilities.

Commentary

This standard maintains the basic policy of former section 1.60 of the 1990 automation standards and is consistent with the statewide court administration structure advocated by Standards 1.11, 1.32, and 1.41. The evolution of automated court applications since 1990 has supported the wisdom of that basic policy. Court automation in general continues to be plagued by difficulties arising from the incompatibility of court applications with other applications in the same court but more significantly with systems operating in other courts, at the state court level, and with other justice entities outside the court system. Available technology now provides tools to support effective interaction among internal court applications and between court systems and external justice systems, such as the state's criminal history repository, abstractors and credit bureaus, and protective order registries. The tools to share and disseminate data do not require the major amounts of time to implement as was once required for building specialized interfaces among specific applications and systems.

The challenges to using technology to decrease manual efforts, to maintain quality data, and to use technology to help make courts more accessible are no longer primarily the technology. The fundamental issues remain those of organizational boundaries and "turf". As technology has grown to meet the demands for interoperability, court organizations have often not taken advantage of the benefits of economy of scale, shared infrastructure, and shared vision. Too often, they continue to operate with a high degree of technological independence, often based on arguments of the need for independence of the judicial branch or of individual courts and of the uniqueness of individual courts and their automation needs. In the technology environment of 2005, it is possible and desirable for courts to plan and use common technologies, infrastructure, and applications without jeopardizing independence. Our experience since 1990 has shown that the "uniqueness" of every local court's automation needs is an expensive and debilitating myth for the judiciary. While court automated applications must be scalable to support large and small court operations in both unified and non-unified court environments, the basic functionality, structure, and capabilities needed within applications are the same from court to court and can be met with -appropriately designed systems based upon open technical standards.

In each state, among states, and with other actors in the justice system, courts must obtain the greatest benefit for every tax dollar spent.

The goal of technology available in 2005 is to make possible highly integrated, inter-connected, and inter-reliant systems based upon mature, interoperable and effective systems that are non-proprietary. The security of the nation requires the justice system to participate in such systems, provided that they safeguard the security of the court's data, systems and processes. The efficient operation of individual courts and of statewide court systems requires the same. But such systems cannot be put in place without common planning, system design, and system operation based upon interoperable standards.

All of the above considerations reinforce the need for state level architecture, standards, and policies to ensure that all applications throughout the state court system interoperate successfully both within the judicial branch and outside the branch with executive branch justice entities.

a. Governance mechanism

The Supreme Court, by administrative order, should establish a governance body composed of representatives of all levels of courts within the state, including judges, administrators, technology specialists, and representatives of the bar and executive branch agencies with whom the judiciary regularly exchanges information. The role of the governance body should consist of policy and priority setting, strategic planning, ensuring compliance with national standards, setting state standards, and monitoring the progress of statewide court automation.

Commentary

Establishment of an effective governance mechanism is essential to effective planning, priority setting, and program implementation. The members of the governance body provide essential input into planning and priority setting. An appropriate governance structure ensures that planning and priority setting is based on direct information concerning the business needs of the trial courts, the bar, and other agencies.

Some states have established governance bodies with only an advisory role, reserving ultimate decision making authority to the administrative director of the courts, the state's chief information officer, and the Supreme Court. The more effective practice is to vest decision making authority in the governance body – giving the courts within the state control and ownership of the court automation program, subject to the ultimate authority of the Supreme Court.

The authority of the governance body should not extend to direct oversight of state level automation staff and their day to day operations, which must be under the direct control of the administrative director of the courts so that s/he can be held accountable for technology development and support meeting the needs of all levels of courts within the state.

b. Statewide automation functions

Certain automated applications should be established and operated by the administrative office of the courts on behalf of all courts within the state.

Commentary

Modern information systems are highly integrated processes. When courts began to automate a generation ago, applications were often "stand alone" – a court's case management information system was an independent, free standing application operated by the local court and not reliant on any other systems other than the local utility companies that provided electrical and telephone services. Often civil processing and criminal processing used separate applications, supplemented with a separate application for processing all financial transactions. That is no longer the case. All modern applications are highly reliant upon, and interconnected to, other applications and systems.

A modern case management system in 2005 is “web enabled” – taking advantage of Internet technology (even though it may operate only on an “Intranet” or other wholly internal court network). An optimal case management system will provide accessible and timely information to attorneys and litigants, including automatic notifications of relevant actions. It will interact with office automation software to receive and generate “intelligent” forms and documents based on case processing stages, reducing the amount of manual data entry required of court clerks. It will interact with a document management system for storing electronic documents. It will reduce the court clerks’ daily effort and increase the reliability of a court’s financial processing, supporting the accurate assessment, collection and allocation of fees and fines as required by law. It will exchange information automatically with executive branch agencies and community service providers. It will assign cases equitably to the judges of the court. It will assist in managing petit and grand jury operations. It will provide data that can be used to analyze resource allocations and to plan for meeting changing needs. It will link to attorneys and private companies to receive and disseminate documents – both those created and filed by parties, and those created and filed by the court. It will provide court data automatically to statewide judicial branch data repositories.

The only cost-effective and efficient way to support these interactions is by centralizing appropriate capabilities rather than having individual courts duplicate the capabilities in order to “talk” to other courts and outside entities. The administrative office of the courts is the appropriate location for planning, developing, and supporting the basic statewide infrastructure to support all courts.

The necessary applications at the state level include:

i. A common means for communicating with the courts and providing access to statewide court information

Commentary

The Internet is the standard means of obtaining access to all business and personal information in 2005 and current indications are that its use will only increase, with no other viable alternative on the horizon. The administrative office of the courts should create and support a uniform statewide Internet access mechanism – such as a “web portal” -- for use by attorneys, litigants, the public, and other entities for communicating with all courts within the state. The public should not have to tolerate a multiplicity of access processes for different courts throughout a state.

A statewide court information access site using Internet technology will include standard support applications for all courts, such as an electronic payment mechanism for paying court filing and other fees and traffic and other criminal fees and fines and filing court forms or other applications for submitting information to courts.

The state court system need not create and maintain an independent access site. The executive branch has established a state web portal in most states, often including a statewide electronic payment application. The independence of the judiciary is not compromised by taking advantage of these statewide capabilities any more than it is compromised by the use of a public telephone system. The court system must ensure that proper levels of security exist to protect the confidentiality, security and authenticity of court information in using a statewide web portal. It must also enter into a formal agreement with the executive branch setting forth "service level agreements" – guaranteed performance and maintenance characteristics of the state system made available to the judiciary – that are acceptable to the judicial branch.

ii. Statewide data repository

Commentary

Basic information pertaining to every case in every court in the state should be maintained in a central statewide data repository under the control of the judiciary. Data should be available from automated processing in trial and appellate court case management information systems. The data repository serves multiple purposes:

> Providing public access to court data and documents. Having a statewide data repository enables the state court system to provide public access to court information from a central source. A central public access process saves the time and effort of local court staff throughout the state that no longer have to answer as many telephone inquiries; it is also more efficient for users of court information, who no longer have to access information from different courts through different processes.
>
> Use of court case management applications as public access vehicles requires thoughtful system design to ensure that information is displayed in a way that is understandable to members of the public. Traditional court applications use codes and abbreviations that court personnel come to understand; plain English is needed for understanding outside the court family.
>
> Electronic court documents must also be accessible through the central repository, subject to policies adopted by the Supreme Court governing public access and privacy for court data in electronic form. For a full

examination of these access and privacy issues, see Steketee and Carlson, Developing *CCJ/COSCA Guidelines* for Public Access to Court Records: A National Project to Assist State Courts (National Center for State Courts, October 18, 2002) http://www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf . A statewide repository ensures consistent application of Supreme Court access and privacy policies.

Currency of data is a critical determinant of the extent of public reliance on the system – essential for decreasing the amount of local court staff time spent responding to questions and information requests. Ideally, data will be replicated on the central repository on a real time basis, as it is entered in the trial or appellate court. When infrastructure does not allow immediate replication, courts should ensure that data is no more than 24 hours old by implementing an overnight batch process, updating all information recorded during a court day after the court closes.

Assembling reliable statewide court statistics. A statewide data repository is an essential component of a modern state statistical reporting system. Assembling statewide court statistics through information prepared and transmitted by the staff of local courts creates inevitable inaccuracies and inconsistencies, as the staff of each court interpret the data requests from the state and their own court data. Effective local and statewide court management depends on consistent data, which requires statewide data standards and policies described below and the automatic updating described above.

Responding to inquiries from the legislative and executive branches and from the press. Having a statewide data repository enables the state court system to be responsive to inquiries from the legislative and executive branches and from the press. It is a best practice for the state court staff to provide local courts with copies of data reports generated from the repository for review prior to their public release. An appropriate policy also sets forth the time period within which local courts must respond. This practice not only allows a court to identify and correct inaccuracies in its own data before it is disseminated, but gives the court advance warning of impending public scrutiny so that it can be prepared to answer questions that may be raised by the data.

Supporting the Supreme Court's governance function. A statewide data repository enables the Supreme Court to know the status of case processing in the courts of the state so that it can perform its oversight and governance functions.

Enhancing Security. With economies of scale,a statewide data repository can provide levels of security, including tamper-evident protections to stored data, at less cost than would be required to provide the same levels of security for full public access to the records in every court within the state.

iii. Statewide telecommunications and training network

Commentary

The administrative office of the courts should be responsible for creating and maintaining a statewide telecommunications network for all courts within the state. In 2005, the most efficient means for most communications within and among courts in a state is through a court "Intranet" – a secure internal communications network using Internet communications protocols.

"Voice over IP" applications enable telephone communications to be conducted over the Internet. These applications can be enabled and supported at the state level using the statewide telecommunications network.

The network should support video conferencing as well as voice and data communications, enabling the state to conduct meetings and to provide training sessions electronically. Judges and court staff can participate in these sessions from their chambers or offices without the cost in time and dollars of travel to a central location.

The statewide network should also include the capability to participate in web seminars, classes, and presentations provided nationally by organizations such as the National Judicial College, the National Center for State Courts, the American Bar Association, and other providers.

A best practice in 2005 is to use statewide court communications networks to disseminate procedures, policies, and standard documentation such as bench books. Internet access to videos that explain bench book materials and practice manuals, provide information to potential jurors, and give answers to common procedural questions for self represented litigants requires a statewide communications network with adequate bandwidth.

iv. Statewide maintenance and support

Commentary

In 2005, it is a best practice for the administrative office of the courts to be responsible for statewide automation maintenance and support that provides economy of scale, ease of use, and access to limited technical expertise in specific areas.

Examples are:

A statewide help desk for common court applications. A central staff can provide support by telephone and video conference for applications used in multiple courts, such as standard case and document management applications, electronic filing, the use of courtroom technology, and even basic word processing applications. Best practices, in 2005, include the use of software to record and monitor completion of all calls for service, the use of software that allows the central help desk staff remotely to assume control of a local court application session for a particular user to "walk" the user through the steps in a process, and automatic "escalation" of problems that are unresolved and automatic notification to the person who reported the problem. This software also allows central staff to remotely upgrade software residing on local court servers and personal computers and to confirm software license validity.

Best practices, in 2005, also call for the designation of and special training for "super users" in each court, who are equipped to answer most basic questions concerning court applications and equipment and are skilled in identifying the questions that need to be referred to the statewide help desk.

Training for common court applications. Central staff can provide standardized, professional automation training to court users through hands-on training sessions for new employees or for new applications, video conferencing training sessions, videotape or CD Rom training materials, and Internet-based training applications. Ideally, applications include "self-test" mechanisms that can be monitored by supervisory staff to ensure that staff have acquired and maintain the skills needed for specific job performance. Best practices, in 2005, include annual training requirements and certifications for court staff, similar to lawyer continuing legal education requirements. Effective training programs require close coordination with "super users" who provide the introductory training to new and temporary staff.

Asset management for all automation equipment. State inventory control requirements impose heavy duties on local court staff to maintain accurate information for every computer, printer, PDA, server, router, etc. Compliance with the terms of software licenses is a requirement of state and federal law, which many local courts are not adequately equipped to manage. State automation hardware and software asset management policies are needed and state level staff can monitor compliance with them and be assigned the responsibility for monitoring individual PC software to ensure legality, using remote access software functions.

Virus, worm, and spam control for all court users. Multiple virus detection software and spam filters should be maintained on a central basis, updated quickly upon receipt of updates, and monitored by state staff, thereby increasing the security of state court telecommunications and data processing applications.

Continuity of operations planning and testing. Best practices, in 2005, include detailed planning for the maintenance of court operations, including, particularly, the maintenance of court automated applications and networks, both for reliable "normal backups" and for protection in the event of disasters. Effective planning includes periodic simulation exercises in which the courts actually operate using the contingency plans and applications. Use of "hot sites," database redundancy at multiple sites, and redundant network capabilities are common resolutions to avoid single points of failure. Continuity of operations planning is often coordinated and supported at the state level, although much of the actual execution and specific planning must be done at the local court level. With widespread reliance on Internet communications with the courts, courts have an obligation to include in their contingency planning notification mechanisms so that those attempting to access information learn of present Internet communication limitations, including temporary limitations on sizes of files accepted, resolution timeframes, and contact information for access to a human information source. Centralized help desks can be the point of contact not only for court staff, but also for the public in such contingency plans.

Replacement and upgrade strategies. Development of statewide replacement and upgrade strategies is essential to ensure that equipment in all courts continues to provide the capabilities needed for local, statewide, and national applications. System life cycle planning takes into account the regular obsolescence of most hardware and software. Even though an application may still function five years after it was installed, the hardware and software vendors may no longer support it with replacement equipment or service, making it impossible for a court to continue to use it. Statewide hardware replacement and software upgrade strategies include budgeting for new equipment, software programs, and for processes for rolling out the replacement and upgraded products, including training of court staff in their use. Performing these functions at the state level saves resources, but requires the use of standard equipment and software.

c. Statewide architectural and strategic planning

Commentary

Automated applications, in 2005, are inter-connected and inter-reliant. Their reliable, consistent, efficient and secure operation requires a sound, commonly applied technology "architecture." Just as an architect's design for a physical structure determines how the various rooms and accesses of the structure will interoperate, how they will be provided with natural light, electrical power, network and telephone outlets, and heating, cooling and air circulation, so also a statewide technology architecture specifies the various hardware and software components of the courts' automated systems and how they will interact and interface with each other. Neglect of this process ensures that systems will not interface as planned and guarantees expensive and time consuming replacement of hardware and software, or doing without desired system capability.

In 2005, the best practice in public sector technology architecture is "service oriented architecture" which creates the flexibility for a court system to interface with multiple different hardware platforms and software products that comply with basic standards allowing interoperability. This becomes increasingly important as courts pursue additional "devices" such as PDAs, multi-function telephones, and other productivity-enhancing devices to allow access to data when court staff are not at their desks.

Strategic planning involves creating a long term vision for the judiciary's automated capabilities, creating the basic infrastructure needed to support them, and sequencing the addition of specific applications and enhancements in a coordinated, efficient, and cost-effective way. Strategic planning, ironically, must also accommodate the rapid changes in technological capabilities and products that inevitably require revision, and sometimes radical revision, of components of the strategic plan. Effective planning, therefore, requires that court technology professionals retain very current knowledge of technology trends and developments that will have an effect on court technology strategic thinking. The most effective means for maintaining that currency is regular attendance at technical conferences and training; not only those provided specifically for courts, but also those provided for general public and private sector technologist audiences. The expense is significant and creates personnel policy issues because the cost of maintaining technical staff currency is significantly greater than the proficiency training costs required for non-technical staff. Best practices, in 2005, include adequate advanced budgeting to be certain that technical staff can maintain their currency; the cost/benefit ratio of these expenditures is justified by the costs associated with technology changes that catch the judiciary unaware.

Strategic planning also encompasses the identification of standards for hardware and software with which all courts in the state must comply, with a migration strategy that gives local courts supported by local funding a reasonable opportunity to plan and comply.

Strategic planning uses the principle of "life cycle cost of ownership" for a system or application, calculating not only the cost of procurement or development of the system, but also the ongoing costs of training and deployment, maintenance and support, licensing fees, operational costs, the "hidden costs" of support by super users, and cyclical replacement of equipment and periodic enhancement of software. Identification of less complex solutions and cost sharing arrangements, especially with executive branch entities, are critical parts of effective strategic planning.

Migration of systems and applications to new platforms and standards are also critical aspects of strategic planning. How to maintain critical operational data, while converting from a legacy application to a new replacement system with enhanced functionality, is among one of the most difficult technical and policy issues that automation planners face. Anticipating migration issues often makes it possible to mitigate the problems encountered.

A well-planned hardware and software architectural foundation mitigates many of these common problems.

d. Statewide data standards

Commentary

A chronic problem for state courts is inconsistent entry of information in case management information systems and basic information entered only as free form text. Within an individual court in which all staff use the same case management application, different court units, and even different staff within the same unit, often use different data entry codes for the same information, often to express only minute differences and even more often as a matter of personal preference. When a court uses multiple applications for the same functions, and when the courts of a state use different platforms and different applications, the obstacles for obtaining consistent and reliable information escalate. Judges, court staff, and lawyers who use case management information as narrative text to describe what has happened in a case are not hampered significantly by these inconsistencies; they are usually able to understand accurately what has transpired even though the entries are not fully consistent from case to case or within a case from one person to another. But when the data is used to produce management reports for the court, when it is used in its electronic form for exchange of information with executive branch agencies or for interfacing among multiple court systems (for instance with electronic filing, document management, and automated workflow management systems), and when it is compiled for purposes of statewide statistical reporting, the inconsistencies and lack of commonly coded data are intolerable.

Creation of consistent and reliable electronic data requires a change in court culture, beginning with the establishment of statewide data standards – defining a single set of codes applicable in all courts with a specific meaning attached to each code. The National Center for State Courts, in conjunction with the Conference of State Court Administrators, has published the *State Court Guide to Statistical Reporting*, which provides basic nationwide standards for the structure and content of case categories, subcategories, and case types. The *Guide* also sets forth fundamental policies, such as the limitation of criminal filings to a single criminal defendant. The *Guide* serves as the starting point for the development in each state of complete data standards, with supplemental content to reflect the state's own structural and processing needs that conform to the standard structure.

The statewide data standards must be dynamically maintained – adjusted frequently to reflect changes in state law and court rules and to accommodate new case management needs identified in the courts. The Supreme Court needs to establish a representative entity, which could be a subcommittee of the statewide automation governance body, to make those decisions in a very prompt manner within a cooperative context that finds solutions for consistency while also allowing for necessary differences between court levels and local practice. Extensive training, creation of data quality assurance processes in each court, and establishment of data monitoring and auditing functions at the local and state levels are needed to complete the necessary culture change.

e. Statewide administrative policies

Commentary

The architecture, strategic planning, privacy and public access policies, and data standards decisions all require the imprimatur of the Supreme Court to make them binding on all courts and court personnel throughout the state. The Supreme Court must be willing to enforce its administrative policies and rules in the face of inevitable local opposition. The support of a representative governance body proves useful in these instances.

Effective automated systems also require more detailed administrative policies on a variety of topics, such as regular changes in passwords, restrictions on loading personal software onto court owned equipment, restrictions on use of the Internet, and restrictions for connecting non-court computers to court networks and applications. Although these administrative policies must be consistent, the consistency must often be established by job function, not solely by making policies the same for all staff.

Although development of policies needs to occur at a centralized level, actual enforcement need not be centralized. Violation of automation policies are best handled by individual supervisors as any other infraction of personnel rules. Security and protection of systems is essential, but should be approached carefully to prevent unnecessary inconvenience.

f. Statewide procurement and licensing

Commentary

Significant cost savings and statewide consistency arise from statewide procurement processes for hardware and software. Large purchases of software licenses are usually accompanied by significant discounts. Similar discounts are available for statewide purchase of automated legal research services. A centralized negotiation of these contracts, regardless of the funding source used for actual purchase, can result in both significant savings on initial purchase and improved processes and savings for on-going maintenance.

Model procurement documents and recommended processes are available from SEARCH (The National Consortium for Justice Information and Statistics) and from the National Center for State Courts. (http://ncsconline.org/)

Procurement documents must reference applicable functional and technical standards. However, those standards must be used with appropriate sophistication. For instance, the case management information system functional standards include both “mandatory” and “optional” items. It is not appropriate therefore to merely require “compliance” with these standards.

g. Statewide support for business process redesign

Commentary

Modern integrated information systems provide great opportunities for improved efficiencies and economies. But those economies come not from implementation of the automated systems, but rather from the modification of existing business practices to take advantage of the efficiencies provided by the new technology. Illustrative examples arise from electronic filing and the maintenance of court records in electronic form: The most significant savings arise from the elimination of traditional paper files; however, judges must agree to dispense with those files. Supreme Courts must designate the electronic record as the official court record, and judges must use documents in electronic form or print them as necessary for a specific activity. Electronic documents can be time stamped electronically by linking them to a separate electronic file stamp; however, court clerks must be willing to dispense with the appearance of the traditional marking in the top right hand corner of the first page of the filed document. Automatic service of filed documents on opposing counsel is easily accomplished through a court’s electronic filing application; however, the court must be willing to re-think the traditional allocation of responsibilities for service in order to take advantage of the opportunity provided by the technology.

In order to take advantage of the efficiencies offered by new technologies and applications, courts and lawyers must alter the way in which they do business. A statewide group of business process analysts can assist local courts in developing changed policies and in transferring improved processes from the initiating court to others.

1.61 Comprehensive court automation applications

The state should ensure that all courts have a core set of automated applications.

a. A case management information system having at a minimum the functionality set forth in the Conference of State Court Administrators (COSC)/National Association for Court Management (NACM) functional standards.

Commentary

The COSCA/NACM case management information system functional standards were developed to provide courts and technology vendors with guidelines for the functionality that should be expected of a modern case management application. The functional standards are available from the National Center for State Courts website (http://ncsconline.org/).

In 2005, the best practice is for a state to procure a single case management information system for use by all levels of courts within the state. The application must be scalable to accommodate the needs of the largest and the smallest courts in the state. Having all courts within the state use the same case management application simplifies enormously the problems of creating standard interfaces with other, statewide applications. However, it does not, by itself, ensure the consistency of data entry, discussed above; methods for quality assurance, data standards, and monitoring of compliance are essential.

A satisfactory case management information system must contain application program interfaces to interact with essential functions as appropriate to the individual courts, such as word processing, electronic filing, payment, financial, public access, document management, jury management, and statistical applications.

b. Standard office automation applications appropriate for each person's duties, including PC or server hosted fax processing, word processing, email, Internet access, spreadsheet, super user data base applications, ad hoc reporting packages, calendar, financial processing, graphics, and project management software.

Commentary

Statewide standards should specify standard office automation applications that every court and every employee of the court system will use in order to obtain efficiencies in procurement and technical support and to support statewide architectural and strategic planning choices.

Variances from the statewide standards should be allowed when specific individuals need multiple applications because they must communicate with other entities who do not use the judiciary's standard applications, for instance, for word processing or spreadsheets.

c. Applications to support an electronic document management environment, including electronic filing, electronic service, electronic access to court documents, automated workflow management, and document and file retention and storage

Commentary

In 2005, numerous courts have converted all or substantial portions of their documents to electronic form. Their experiences have identified, addressed and solved many of the basic impediments that previously stood in the way, including questions of archiving documents in electronic form. Standard 1.65 addresses electronic filing and the issues associated with it.

Conversion from paper to electronic documents requires significant changes in a court's business practices. The most profound is that a piece of paper is no longer available to move from place to place within the court to inform judges and staff that an action on that paper is required. Automated workflow management applications make the same transfers automatically, causing documents and associated messages to appear on a "work queue" on the appropriate judge's or court staff member's computer screen. Imaged documents alone do not provide the needed data to drive workflow, to generate court documents, or to provide statistical information. Standard data entry remains essential for accurate functioning of automated workflow management applications.

Electronic filing applications within the same state should be accessible through the statewide access called for in Section 160(b)(i) with the same electronic interface so that attorneys, law firms, and other court users need to learn to use only one set of electronic procedures.

d. Standard courtroom technology, including audio amplification and recording, video recording, video and telephone conferencing, evidence presentation equipment, and display monitors and screens for the judge, courtroom personnel, attorneys and parties, jurors, witnesses, and spectators.

Commentary

Every courtroom should be equipped with the technology needed to conduct video arraignments, telephone and video conferences for remote presentation of legal arguments and witness testimony, for interfacing with media cameras, and for counsel or parties to use audio visual aids in presenting evidence and arguments. Evidence presentation equipment includes a document camera, VCR, CD Rom, and DVD readers as well as access for counsel-provided presentation software. Courthouses must have the wiring and structural infrastructure to support these courtroom applications and others that will undoubtedly be developed in the near future, and if wireless access is enabled, it should be suitably secured.

In 2002, the Judicial Council of California promulgated *Facilities Guidelines for Technology in the Courthouse* which describes in detail the technologies set forth in this standard, and the necessary supporting infrastructure. The Courtroom 21 Project at the College of William and Mary in Williamsburg, Virginia provides current advice and assistance in the application of technology in the courtroom (http://www.courtroom21.org).

e. Statewide and local court websites, including information about the court system, information about the court's rules and processes, access to statutes and court precedents, fillable forms, access to public data in the repository, instructions for persons representing themselves, electronic filing and payment process, calendar access, and court performance and workload data

Commentary

Websites have become the preferred method for disseminating information about the court system and materials to assist persons in accessing court services. It is not only preferred by the courts, because accessing its information requires no staff assistance and entails no printing costs; it is also preferred by court users, who are able to access and print information from their homes, offices, libraries, or community centers. A leading example in 2005 is the California state court website and its self help information, including fillable forms and other advanced components. See http://www.courtinfo.ca.gov. See also Maryland's People's Law Library (http://www.peoples-law.info/Home/PublicWeb) and Alaska's Family Law Self Help Center website (http://www.state.ak.us/courts/selfhelp.him).

Courts are sometimes cautious about reliance on technology because of concerns about equal access – concern that too many litigants will not have access to a particular technology. However, **t**he "digital divide" does not appear to detract significantly from the utility of court websites. Studies in Alaska and Minneapolis, Minnesota found that 85% and 70%, respectively, of self represented litigants reported that they had access to the Internet to obtain court information and forms.

An important development, in 2005, is "document assembly" applications that obtain information from a potential filer in the form of an interview questionnaire and then, based on the information provided, choose and complete the appropriate form for printing and filing or for electronic transmission to the appropriate court.

f. Access to automated legal research

Commentary

A basic component of the automation needs of judges, law clerks and other court staff attorneys is access to automated legal research tools and services. In 2005, most statutes and many reported appellate decisions are being provided by state governments on the Internet free of charge.

g. A jury management application

Commentary

There are no national functional standards defining the desired components of jury management software, which should be provided to all courts in which jury trials are conducted. Such software should have the capability to merge source lists and eliminate duplicate records, randomly select panels of potential jurors, generate juror summonses, automatically scan information from returned juror qualification forms and questionnaires, record and analyze juror demographic information, assign jurors randomly to jury venires, produce juror courtroom seating charts, record jury disqualifications, excusals, challenges for cause and peremptory challenges, record jury service, schedule juror postponements and generate summonses for them automatically, and handle juror fee and expense payments.

This functionality may be found within some case management information systems.

h. Automated applications for recording and maintaining the court record

Commentary

Courts use a variety of methods for preserving the court record, including court reporters and voice writers (including "realtime" reporting), audio, and video recording. Automated applications exist to support every mode of preserving the court record. Such automation should be used in court reporting activities. To protect the integrity of the court record, the equipment and software should be purchased by, and belong to, the state. Reporters should provide the court with electronic copies of the records they make, together with regularly updated versions of the "dictionaries" that they use with their transcription equipment. Such copies and applications should also be closely monitored for security issues involving data integrity and authenticity.

i. Administrative applications

Commentary

Courts need automated applications for financial, personnel, inventory, archiving and facilities management. These, like other applications, should be provided centrally by the state court system.

j. Applications to support ancillary court services

Commentary

When courts are responsible for other services, such as adult or juvenile probation, pretrial services, home studies, mental health services, or alternative dispute resolution services, these services should be supported with appropriate automated applications, procured and maintained on a statewide basis when the services are provided by all or most courts statewide.

1.62 Information sharing with other justice entities

Courts should obtain as much information as possible in electronic form from executive branch agencies and lawyers and provide as much information as possible to them in electronic form, following accepted industry standards.

Commentary

Recent developments in technology have reduced dramatically the practical and political barriers to electronic information exchange between the courts, lawyers, and executive branch agencies. In the past, the only practical means for exchanging such information was for courts and executive branch agencies to use the same automated systems; concerns about separation of powers and the independence of the judicial branch of government made such shared systems exceedingly rare. In the recent past, exchanges of information between independent, autonomous systems became technically possible, but automated interfaces had to be negotiated and built individually for every information exchange, mapping the data elements between the two exchanging data bases. Any change in the data being exchanged required rewriting the interface software, a costly, time consuming, and tenuous process.

The development and widespread acceptance of eXtensible Markup Language (XML) has changed the landscape dramatically. XML uses standard "tags" within a standard syntax to create a common reference point to which a court can build a single interface and be able to exchange information securely and satisfactorily with multiple entities using the same XML standard.

It is now technically and economically feasible for courts to obtain criminal and traffic charging information electronically. It is possible to provide criminal conviction and warrant information electronically to law enforcement and corrections authorities. It is possible to provide automatic notification of probation officers when a probationer is arrested. It is possible to exchange real time information with child support enforcement agencies, domestic violence prevention programs, child protective services, and motor vehicle departments. It is possible to provide real time scheduling information among courts, prosecutors, public defenders, probation departments, sheriff's offices and private attorneys. These exchanges are not only possible, but highly desirable. Direct entry of information from one data base to another eliminates not only delay in transmission of the information and the cost of keying the same information multiple times; it eliminates altogether the error rate in information entry making possible clear accountability for information quality by the entity responsible for its initial creation and entry.

The Global Justice Information Sharing Initiative, a formal advisory committee to the US Department of Justice, in 2004 issued the first releases of a Global Justice XML Data Model – an XML schema containing several thousand justice system data element names within an object model. The data elements are "normalized" – defined at a level of specificity that allows technical staff to be certain that they will not needlessly repeat data that has the same meaning in a data exchange. The US Department of Justice and the US Department of Homeland Security in 2004 required the use of the GJXDM in all information systems supported by federal funding from their agencies. XML will be the future basis for states to provide criminal arrest and conviction records to and obtain criminal history and other background information from the FBI's National Crime Information Center.

This standard is intended to encourage electronic exchange of justice system information as rapidly and widely as possible, using standard information exchange tools.

1.63 Development and support of automated applications

In developing new automated applications, courts should follow these best practices:

a. Courts should insist that their applications comply with nationally applicable standards

Commentary

In August 2001, the Conference of Chief Justices adopted a resolution calling on all courts of last resort or judicial councils in the states to require "courts within their state

> a. to comply with applicable national communication protocols and standards when procuring or developing new electronic filing and information-sharing systems or when adding these functions to existing case management information systems;
>
> b. to comply with applicable national standards when procuring or developing other new applications, unless there is compelling justification not to do so; and
>
> c. to comply with, or migrate toward, applicable national standards when enhancing existing applications."

The resolution recognizes that the purpose of national standards is to ensure national interoperability of communications systems and to set expectations for the functionality to be provided in case management information systems.

b. Courts should take advantage of open source and public domain software when possible and practical.

Commentary

This section is not intended to apply to operating systems, networks, browsers, email, or standard office applications such as word processing, spreadsheets, and presentation or publishing applications. Courts will continue to use commercially developed and proprietary licensed applications in these areas. Judges and court staff are familiar with these commercial products, they are widely accepted throughout the public and private sectors, support and upgrades are readily available for them, and large numbers of other products are designed to interact successfully with them.

However, while courts will continue to use commercially developed and licensed software for many purposes, they should remain aware of opportunities to use public domain and open source software and applications when available to meet a particular need.

Software created by courts is usually considered to be in the public domain. There have been surprisingly few instances in which courts and states have made use of already developed software applications. Yet there is at least one successful example of state court adaptation of software developed by a federal court in the same state; the state of New Mexico modified an electronic filing application developed by the United States District Court for the District of New Mexico for its successful pilot electronic filing application.

Open source software has become more available in recent years. Several electronic filing components have been developed using open source processes and licensing, including OXCI, the Open XML Court Interface, designed to link document assembly applications with court case and document management applications.

c. Courts should exhaust all possibilities for using or adapting public domain, open source and commercial software products before deciding to build their own software applications

Commentary

The buy, adapt, or build decision is a persistent issue in development of court automated applications. Technology staff, often prefer to build and maintain their own applications – it is the most stimulating, challenging, and rewarding technology task for a trained professional – much like arguing a case before the US Supreme Court for an appellate specialist. However, internal software development from scratch often presents a myriad of challenges.

Before court technology staff can undertake development of software internally, they must gain an intimate understanding of court operational processing to avoid underestimating the complexities of needed applications, including the cost and time required to deliver the product. Also, court technology staff must make painstaking efforts to document their software so that other technical staff can maintain and enhance it in the future. Courts often have difficulty retaining automation staff; when a developer leaves the court staff, s/he may take the only expertise available to support and maintain the systems s/he designed and built. Other costs that states and courts must analyze and consider before they consider building their own software applications are:

- The expertise required to make strategic choices among available software and database architectures on which to base a new software product;
- The costs of technical training for court programmers to develop and maintain their competence and their familiarity with new programming languages and approaches;
- The expertise required to manage a staff of programmers;
- The project management expertise required to complete software development, testing, training and installation within a fixed budget and project time frame;
- The "fully loaded" costs of technical staff, including the costs associated with staff turnover, temporary vacancies, and the learning curves for newly hired replacement staff;
- The need for application analysts to develop and document detailed systems requirements to guide the efforts of programmers;
- The time of operational staff needed to assist in requirements definition and testing; and
- The opportunity costs to the court of waiting additional years for a software product "built from scratch."

Using available public domain, open source, or commercial software allows courts to "share" the technical development and maintenance costs of creating and enhancing software. Considering the total life cycle cost of ownership, adapting existing available public domain or open source software, or licensing commercial software from a reliable and stable court technology vendor, normally provides the court with the best return on its resources by leveraging investments already made in existing products, reducing the risks of time and cost overruns, entitling the court to future enhancements and upgrades developed by or for others, delivering a proven product, and providing future support for that product without the need to maintain a large group of programmers on the court's payroll.

An argument often used to justify the decision to build rather than to adapt existing public domain or open source software, or to buy a commercial software product, is that the court can obtain an application that exactly tracks the court's current business practices. However, replicating existing processes deprives courts of one of the primary values in new automation – fostering re-thinking of the reasons and needs for current business processes. Consequently, this justification undercuts one of the principal benefits of a new application. It also tends to prolong the development cycle as court users demand successive modifications of the software to get "exactly what we want to support current methods of operation."

Courts should build their own applications only when no acceptable public domain, open source or commercially supported product exists. The adjective "acceptable" as used in this commentary is intended to describe the required basic functionality of the software application, not the exact way in which the functionality is delivered by the commercial product. It is often possible to replace or upgrade the user interface for an application (the actual screens seen by users, the way users interact with those screens to obtain and to enter information, and reports generated by the application) while taking advantage of the basic structure and functionality of an existing application. Courts should also be willing to consider changes in procedural rules, as well as local operating practices that may be required to import a software application successfully used in another state or court.

d. Courts should require software vendors and court staff to use a “spiral” development process in producing and enhancing new applications

Commentary

The traditional software development process called for in the 1990 court automation standards is now referred to as the “waterfall” process. Under that model, design and development proceed in a linear, highly structured fashion. The court defines its requirements at a very high level and then at a very detailed level and the software developer then builds and tests the application against those requirements. Inevitably the court ends up disappointed in the product, even though it may fully comply with the original requirements the court itself developed. Users are never able to envision fully how they will use an application before they actually use it in their daily work. As soon as the first court user uses the application for the first test case, s/he sees a better way for the system to work than the way specified in the requirements document. However, if the end product has already been defined by the requirements set forth by the court, the modifications will be time consuming and very costly.

The “spiral” development process was developed in response to the repeated failures of the “waterfall” model. The original requirements are developed at a relatively high, general level, with the primary concern being ensuring that the technologists can develop the systems structure, the database structure, and design to support the myriad court requirements. The developer creates a “prototype” application with only the basic functionality called for, without refinements. The prototype is tested and critiqued by court users. The court system and the developer negotiate refinements to the requirements based on actual experience with the prototype. The developer produces a second prototype, with increased functionality, which is subjected to another round of testing by end users, with further ensuing refinements. Software development languages have become so sophisticated and flexible that significant changes in software functionality can be made by a knowledgeable programmer in short order and at modest cost. The spiral development process continues for multiple iterations, with the prototype moving ever closer to the final product, which is then delivered and installed.

However, the developer continues to refine the product after its initial use, with the frequency of change decreasing over time. The most important insights about possible changes to business processes occur only after the new software has been in use for a few months. The developer must be willing to continue to revise the software code quickly and at reasonable cost over the product’s life. The danger of the “spiral” model is that the process may be indefinitely prolonged as the product goes through repeated iterations. Effective management of a "spiral" development process requires the discipline to deploy a "less than perfect" product, knowing that additional refinement will continue to occur.

Service Oriented Architectures – which call for the reuse of functional modules across multiple software applications using "loosely coupled" software engineering approaches – provide a mechanism for speeding the development of software using the "spiral" model.

1.64 Security

Courts should employ sufficient architecture, applications, and procedures to minimize recognized threats to the security and integrity of court data, documents, and processes.

Commentary

Security is a major component of the design, implementation and maintenance of court automated systems. While no automated system can be made completely secure, the most likely threats can be thwarted and breaches of security that do occur can be detected and countered.

Best security practices in 2005 include, in priority order:

<u>Continuity of operations planning and testing</u>

This topic is discussed in Standard 1.60 (b) (iv). Continuity of operations planning is an essential component of automation security. Effective continuity of operations planning takes into account the likely failure of utilities, telecommunications facilities, and interconnecting networks and applications. One of its principles is to ensure that there are multiple independent routes by which messages can be transmitted and received and that courts can perform rudimentary data entry and reporting functions when cut off from interconnected systems.

<u>Backups and off-site data storage</u>

The most basic form of computer security entails the maintenance of backups of all data. Traditionally, server and database backups occurred daily, during non-business hours, with routine processes to maintain proper sequencing of daily, weekly, and monthly backups to ensure that data could be restored from a "good" source even if a data corruption problem was not identified for several days or weeks. Modern server and database backup procedures can be conducted almost instantaneously, copying all database changes to a replicated or mirrored database maintained on a separate server.

Redundant copies of data in a single location are not adequate for security. Off-site storage is essential to ensure continuity of operations in the event of physical damage to the courthouse. Replication of data to an off-site computer can now be accomplished electronically.

The proliferation and dependence on personal computers has increased the need for individual personal computer backup processes to supplement centralized server backups. For example, most servers do not save email once it is downloaded from the server; staff may not regularly save draft documents or correspondence on servers, particularly if they use laptops that are frequently not attached to the court's network; and staff are often encouraged to delete unnecessary files on the court's servers to avoid the need to purchase additional central storage media. Recent technology advances have removed the onerous and time consuming efforts involved in personal computer backups; options for backing up and storing 5 G to 100 G of data on small, relatively inexpensive external media are now available, allowing incremental copying of only the data that has changed since the last backup. An additional benefit of these small personal computer backup media is that files can be accessed from a different personal computer; if a staff member's personal computer fails, s/he can continue working from another computer, using her or his files stored on the backup media.

All of a court's central and local backup processes must be tested periodically. Often in the past, courts have identified flaws and gaps in their backup routines only when they first tried to use backup data to replace lost or corrupted data.

Maintenance of sound personnel practices and supervisory oversight

Most serious security breaches occur because of the actions or inactions of court employees, through sabotage, criminal action, or failure to follow security requirements. An aggrieved employee may purposefully destroy or alter court data. An employee may falsify court records for compensation. An employee may give an administrator password to a hacker. An employee may upload personal software or files containing a worm or virus onto court equipment, infecting the entire network. An employee may forget to lock a public door, leading to theft of computer equipment containing confidential court data. These "low tech" risks are the most serious ones that a court faces. Court technology staff inevitably have access to all court records, data and passwords. The court must be able to rely on their honesty, integrity and good faith. These risks cannot be eliminated. They can be minimized through sound management and supervisory oversight and by insisting on compliance by all staff with security procedures and requirements.

Maintenance of the currency of software patches for basic applications and the currency of virus checking profiles

Data can be destroyed by computer viruses and worms. Studies have shown that most virus damage is done days or weeks after the virus first appears and well after effective software patches and anti-virus definitions have been made generally available. Employees have neglected to install the available patches and to download new virus definitions. Rigorous discipline in these basic security procedures significantly reduces known risks to court data bases.

Constant threat monitoring

Software is available to report all alterations to data bases, the user ID or IP address of the modifier, and the time of alteration. Use of this software and careful, daily attention to its reports will disclose unauthorized manipulation of court data and allow the revoking of user authorizations used to gain access or other countermeasures to prevent future intrusions. Such monitoring also enables court staff to reinstate the prior version of the data and to rigorously check the accuracy of the records accessed.

Firewalls, Virtual Private Networks, and Network Security

Firewalls and Virtual Private Networks (VPNs) protect access by anyone other than authorized, recognized users and also allow for controlled access to outside websites to limit the possibilities of threats from such sources. These are highly effective and widely used security features. They should be used in conjunction with other security software that identifies attempts at unauthorized access or execution of unauthorized programs by shutting down court systems – or access to them – to counter such threats. Courts may use multiple firewalls to provide different levels of security, with some databases stored outside the secured internal court firewalls to allow public access to selected data.

The proliferation of wireless connectivity has increased the need for security controls on personal computers with wireless access; smart cards and other biometric devices now exist to provide additional layers of protection so that wireless access to hardware and data can be more reliably limited to properly authorized users. Although security features are improving, in 2005 wireless communications remain more prone to undetected intrusion than wired connections. Therefore, courts contemplating the use of wireless solutions should conduct a separate threat analysis prior to implementing a wireless network for any purpose. Appropriate software, hardware, training, and personnel are needed to diminish the threats associated with exposing the court's hardware, networks and data to tampering through wireless communications.

Network security is accomplished by a combination of hardware (such as routers) and network software. Redundancy is desirable in ways similar to those used for duplicate data storage – multiple routes to each point on the network that allow for alternate routes if the "normal" route is compromised. Courts are finding they need specialized staff to prevent, monitor, and correct network security breaches.

Use of "hashing" algorithms to detect alterations to documents

The National Institute of Science and Technology has promulgated a family of - standards d for creating a unique electronic " thumbprint" or digest of an electronic document. If the document is altered in any way, the "thumbprint" – which is composed of digits and characters that are unique to each text or document being digested, called a "hash" – will change. The electronic filing standards call for the use of such hashing for all official court records. The federal courts include a hash on the acknowledgement of receipt of the filing returned to the filer, so that the filer as well as the court has a record of the hash. Should there ever be a question concerning the authenticity of the document, a new hash can be captured and compared to the original to determine whether the document has been tampered with in the interim Court applications can routinely apply a standard hashing algorithm to a document every time the document is accessed, comparing the hash against the original hash of the document, to determine if changes have been made to the document in the interim. Assuming that there has been no substitution of the original hash, the ongoing integrity of hashed court records can be assured. However, hashing technologies are susceptible to hash substitutions and other attacks and may be considered vulnerable unless combined with encryption to form tamper-evident seals or with preservation of redundant copies of hashes.

Use of digital signature and encryption technology

One way to prevent substitution of the original hash of a court document that is used to make comparisons with later versions of the same document is to encrypt the hash with an encryption key. An encrypted hash is much harder to substitute because the attacker needs the encryption key in addition to the substitute hash. Encryption enhances the security of the stored hashes when used to assure integrity of court documents and records.

Encrypting a hash with an asymmetric key results in what is called a digital signature. With regard to stored court records, each time an encrypted hash or digital signature is accessed, it is first decrypted using a key. In this way an ongoing comparison of hashes occurs more securely.

However, using asymmetric encryption, if the underlying hash is compromised by cryptographic attack, the digital signature may be compromised as well. In 2004 Chinese cryptographers succeeded in breaking shorter hashing algorithms, which indicates that hashing and asymmetric digital signature technology must make substantial advances in the next several years or court records may become vulnerable.

A different type of digital signature uses symmetric encryption instead of asymmetric encryption.[1] This type of digital signature is not vulnerable to the Chinese attack and may be a better candidate for stored court records. Message Authentication Codes and

[1] Symmetric encryption uses a single key to perform both the encryption and decryption functions. Asymmetric encryption uses two keys to perform the encryption and decryption functions. The keys are mathematically related but possession of one does not enable learning the properties of the other. Asymmetric encryption evolved in light of the problem of key transmission associated with symmetric encryption where the encrypting and decrypting parties were geographically remote. A single key could be captured by an attacker during transmission. Therefore, having two keys was considered safer. One was used to encrypt information and the other was used remotely to decrypt it. Asymmetric key usage is fascinating and complex, and is outside the scope of this commentary. Generally, symmetric encryption is faster and impacts server performance siginificantly less than asymmetric encryption. Because many of the automated operations of a court do not involve a need to transmit encryption keys to or from remote geographical locations, symmetric encryption is generally superior to asymmetric encryption for many court automation needs.

Extensible Key Infrastructure use symmetric keys with hashing algorithms to provide such types of encrypted hashes that are immune to the Chinese attack on shorter hashing algorithms and they are thus superior for stored court record purposes.

Where asymmetric digital signatures are affixed by individuals or machines, the digital signatures may also optionally include digital certificates from certificate authorities that identify the person or machine that affixed the signature. This feature is useful where automated identification of the source of the document or message received by the court is necessary. However, one drawback of digital certificates is that they must be checked for revocation each time a document is received, which is a computer intensive task that can unacceptably affect performance of court servers. Also, digital certificates typically expire after one or two years, after which time a check of the digital signature on a document can falsely indicate that the signed document has been altered. This shortcoming renders digital signatures using digital certificates unsuitable for long term archiving of court records.

Symmetric digital signatures in document repositories offer much better long term archiving solution for court documents that must remain tamper-evident for long periods as they do not suffer from these shortcomings.

Black Letter and Commentary of Revised Section 2.80

2.80 Trial court responsibilities for court automation

The trial court is responsible for day to day operation and maintenance of all of its automated applications. To the extent that the court operates hardware and software different from that supported by the administrative office of the courts, the court is responsible for support of that equipment and software.

Commentary

Introduction to the 2005 revision of the standards relating to court automation

Standards 2.80 through 2.83 were adopted by the American Bar Association in 1992. They were intended to identify the technology that should be made available to every trial judge. When they were developed, the drafters identified the equipment and software then available and applicable to trial court judges. Thirteen years later that listing is woefully inadequate; it contains no mention of the Internet. Despite the vision and forethought of the drafters, the current standards are now completely out of date, and largely inappropriate.

The 2005 revision has been prepared with this experience in mind. The drafters of this revision are under no illusion that this work will have more durability than that of the 1990 drafters. The pace of change in technology continues to be astonishing. This revision makes no claim that the concepts presented will be any more enduring than the 1990 version of court automation principles. The drafters, therefore, have attempted merely to set forth the "best practices" and ideas as we understand them in 2005.

Because the court automation applications that should be made available to trial courts and trial judges have been enumerated in the amendments to the Standards Relating to Court Administration, the scope of the court automation discussion in the Standards Relating to Trial Courts has been changed to focus on the role of trial courts in developing, supporting and maintaining court automation equipment and applications.

The only way in which these standards can be of continuing value is for the American Bar Association to revisit and revise them no less frequently than every three years. The maintenance of obsolete standards – in this and in any other area – is likely to cause more harm than good. Consequently, in putting these revised standards forward for adoption by the Association, the Judicial Division recommends the Association revisit this topic no later than the beginning of 2008.

Standards 1.60 through 1.64 of the Standards Relating to Court Administration set forth the role and responsibilities of the Supreme Court and the administrative office of the courts in supporting court automation throughout the state. This standard assumes that the state is performing those responsibilities and details the corresponding role of the trial court.

Trial court staff are responsible for the day-to-day operation of the court's hardware and software. They provide routine maintenance, such as backing up court data bases, enforcing security procedures, installing hardware and installing new or updated software that cannot be installed remotely by administrative office staff, troubleshooting equipment failures, replacing failed equipment with spare machines and sending the failed equipment for repair or obtaining permanent replacements if repair is not possible or advisable, asset management in accordance with state policies, and handling routine equipment problems such as major paper jams in printers. The state must provide adequate training for these tasks; court staff must have the time available to perform these functions as a major portion of their duties.

If a trial court implements an application not supported by the administrative office of the courts, it is responsible for the full range of maintenance, documentation in accordance with state standards and policies, and support of that equipment and software, including full life cycle maintenance and migration of the system to a new environment when the current hardware and software become obsolete.

The trial court is responsible for providing the time of selected court staff to serve as "super users" to provide short term training and to answer basic questions about the use of court applications.

The trial court is responsible for the quality and comparability of its data and for compliance with statewide data standards. A data quality control function is a necessary ongoing role for trial court automation staff. This function involves regular review of case records to ensure that they are maintained consistently and in compliance with standards. The function needs to be performed by an automation staff member with extensive court operational experience.

The court is responsible for designing and generating its own management reports – beyond the standard reports provided by its case management information application – for effective management of all cases pending in the court.