



Technology Integration of the Modern Courthouse

*Common practices for maintaining a reliable
and secure computer network*

Introduction

The implementation and use of a computer network is absolutely essential in the effective operation of an Iowa courthouse or county administration building. From the sharing of data among departments, to the distribution of key data between counties, networks have created an unprecedented new level of potential for file sharing and communication within the governmental realm.

With this potential, however, comes a series of fundamental givens that must be always be considered:

- Network security from internal and external threats is absolutely critical.
- The Internet is pervasive, and citizens expect to interact with county offices via the Internet.
- Technology constantly changes, as must the technology vision of any organization.
- Patrons are beginning to need use computers to access the data they need while at the courthouse because information is stored digitally, as opposed to accessing the data on paper.

With these certainties, teamed with the reality that computer networks are essential in county government, counties are faced with a tall task. Providing its departments with seamless yet secure access to data via local and wide area networks, while monitoring and ensuring the safe exchange of this data within and outside the county network, is a highly-technical process. The process requires the integration of meticulous planning and careful implementation with ongoing practices, to ensure the long-term viability of a computer network.

Through years of experience in providing network service needs to various Iowa county courthouses and many large corporations, the computer network technicians at R & D Industries, Inc. have developed and imple-

mented practices that have proven highly effective time and time again.

The following white paper describes many of these practices. As you read further, you may come across issues that have proven problematic at your courthouse, or which may not have even been addressed. These are issues of that we would be happy to assist you with.

Network Planning & Vision

The key to maintaining a reliable and secure computer network begins with decisions made early in the system's planning and development phase. Once implemented, it remains an ongoing process that includes hardware replacement, software upgrades, a heavy dose of budgeting, and the vision to see and plan future network enhancements and requirements.

R & D Industries offers government network consulting services that include working with clients to ensure their success as they tackle this difficult ongoing process.

Our consultants take a holistic view of computer networks. They maintain the right level of vision to assist your county as it takes its computer network into the ever-changing future. Their services include network architecture planning, security policy planning, assistance with fundamental operation system selection, upgrade planning, assistance with software selection for core applications, procurement services, and budgetary planning assistance.

Network Architecture

Computer networks are the result of meticulous planning and the complex integration of several components. While many of these components may be similar from network to network, each system is structured and designed to fulfill a particular need for the client. These networks remain unique in

Network Planning & Vision

Maximize Network
Reliability

Network System Security

Document Imaging

The implementation and use of a computer network is absolutely essential in the effective operation on an Iowa courthouse or county administration building.



Technology Integration of the Modern Courthouse

vision, structure, and adaptation to a client's environment.

In providing our network architecture services, our system engineers strive to help our clients find their particular network's needs. Whether a county government client's needs dictate the development of a wireless network, or a network with the capacity for VLANs, routing, multiple locations, or remote users, we assist clients in determining what is best for them.

Once needs are analyzed and goals outlined, our engineers can then design a network for your county that meets each of these needs and goals. Our staff can then work to implement the network and help to maintain it through the availability of long-term service contracts.

We can also design and implement network monitoring solutions which can monitor all traffic on a network, and create graphs of network traffic, errors, availability (a test to see if the network is working), etc. We commonly implement network monitoring in larger networks so the network can monitor itself for errors and notify network administrators if anything goes wrong.

Procurement Services

In our modern world, county clients no longer have to go through a technology distributor to order hardware and software for their networks. Government organizations can now receive special government pricing for much of their equipment needs. The challenge lies in ensuring that the items ordered for either new or already existing networks are the right items for the job. Too many times we have seen people incorrectly purchase a piece of equipment for a job, and then later find that correct planning and better vision would have saved them both time and money. We commonly see people get 'exactly the right price on, exactly the wrong thing', we can help prevent this.

Everyday, the network technicians at R & D Industries assist clients in selecting the right equipment and software for a project or upgrade. When making a selection, we make certain clients consider more than just their current needs. Together we look at equipment longevity, future

trends, and potential applications for the items in question. We also discuss how the implementation of a piece of hardware and software can affect the rest of the network either positively or negatively, we consider compatibility, cost, warranty, reliability, as well as security and other factors specific to the situation.

When the correct equipment is chosen, counties can order the pieces through their state contractor, and R & D Industries will charge a small procurement fee for the assistance, which we provide, thereby giving the county both the peace of mind and excellent value.

Financial Planning & Lifecycle Analysis Planning

Anyone who has budgeted and planned for the development and maintenance of a computer network system understands the complex depth involved with the process. When planning for the future of a computer network, a number of issues must be factored into the equation: the lifespan of hardware, advances in hardware, software upgrades, general maintenance costs, change in use, licensing issues, fiscal vs. calendar-year costs, etc. If left unorganized, annual technology costs can become overwhelming as scheduled maintenance costs are put off from year to year. Fortunately, the network consultants at R & D Industries have it all organized for our clients in a single chart which allows for easier technology and financial planning.

The chart, called a Gaant Chart, brings together all of the factors listed above and places them into a single, simple-to-comprehend visual element. The chart lists each set of assets which exists into your network, lists annual costs for upgrades, maintenance and replacement, and provides clients with a window within which they should budget these projects. County offices can utilize the Gaant Chart to budget for technology years into the future, allowing them to maintain reasonable annual costs. Furthermore, this takes the guesswork out of planning and allows more accurate budgeting.

Maximized Network Reliability



Technology Integration of the Modern Courthouse

While the proper use of a computer network greatly improves the efficiency of data sharing and communication, our heavy reliance of this tool requires that it remain stable and resilient.

As stated at the beginning of this document, "the implementation and use of a computer network is *absolutely essential* in the effective operation of an Iowa courthouse or county administration building." While the proper use of a computer network greatly improves the efficiency of data sharing and communication, our heavy reliance of this tool requires that it remain reliable and resilient. *In other words, in a modern courthouse, when the network is down, everyone is in trouble. Employees cannot work and patrons are not served.*

Here are some of the steps we take to make that a reality:

Implement Anti-Virus Solutions

Requiring that a network maintain an anti-virus solution is certainly not a novel idea these days. The goal, however, is to create a system which views anti-virus as a process and not just a step in the process. In other words, purchasing anti-virus software isn't enough. This software must be continually updated to offer your network a final line of defense for eliminating the virus threat. To ensure the integrity of this line of defense, these updates must be done daily.

With the number of workstations receiving email and accessing the Internet at a courthouse, however, it remains difficult to monitor each of these workstations to ensure anti-virus software is updated daily. Therefore, our engineers offer our customers anti-virus systems that work on a day-to-day basis *without user intervention*. This saves a huge amount of labor and massively improves network reliability. Operating on a server, these systems operate independently to download anti-virus patterns from the Internet. They in turn update each workstation and server on the network *automatically*, eliminating the threat of human error in your network's protection against computer viruses.

Implement Group Policies

When it comes to the everyday maintenance of a computer network system, the enforcement of policies and standards about use and configuration of workstations is critical. Workers must retain the

ability to utilize their workstations for a number of operations required for their position, but the installation of software or workstation configuration should be left to others in who have been specially trained and understand the impact of installing software as it pertains to network security and impact on other applications. The implementation of group policies in Microsoft Active Directory ensures that this practice remains consistent.

Microsoft Active Directory allows us to create 'groups' of users and assign specific permissions to each of these 'groups'. Then when a person from the group logs onto a workstation, the network determines who they are, what group they belong to, and therefore, what they are allowed to operate, change, install, etc., on their workstation.

Group policies are valuable in eliminating such acts as the installation of SpyWare software onto your network, the changing of security options in an Internet browser, and reconfiguring their workstations. This ultimately results in higher system reliability and lower maintenance costs through the enforcement of these standards. In summary, group policies allow centralized control of policies to protect your computers and prevent mis-configuration, thereby saving you money on unnecessary maintenance.

Implement Login Scripts

While requiring a login and password in order to access a computer network is a security safeguard, it also can be a means of increasing consistency and ease in the access of pertinent data on the network. Through the implementation of login scripts, the network can recognize each individual user and point them directly to the information both they and people within their department require.

Login scripts can be implemented to accomplish a number of tasks. When users log into the network, drives are mapped to shares on the server as well as to printers a particular user should use. Other maintenance operations and system configurations can be performed using login scripts, resulting in the enforcement of consistency within departments. Having everything work as expected each time a user logs in, saves

Technology Integration of the Modern Courthouse

money.

In a courthouse setting, login scripts will ensure, for example, that those who work in the treasurer's office are directed to the treasurer's data stored on the server upon logging on, while those in the assessors office, upon logging on, are directed toward their own department's data on the server. This simplifies computer operation for county employees.

Implement Network Security

As outlined later in this document, the implementation of several levels of network security can, and will, increase the reliability of any network. Thereby, helping to ensure seamless productivity within each department while protecting your critical data.

As part of our overall network security plan, we implement strong password policies and create user groups for each department. While login scripts direct users in each department's data on the server, we can further limit their ability to access data from the server which is either confidential or is not needed in other departments' day-to-day activities. *This is especially important in protecting private healthcare information (PHI) stored on the server.*

Network Security

Every modern county has spent literally hundreds of thousands of dollars on technology to date, and they all understand their need to protect that investment. Furthermore, each county's investment in talented personnel who rely on this technology in order to perform their daily duties must also be protected. An insecure computer network system compromises both of these investments, limiting the ability of both your network and your personnel to work properly.

And what about the information stored on your network? This information not only represents thousands of hours of work, but also critical information and records that cannot be duplicated.

The network technicians at R & D Industries approach the issue of network security from all angles, taking a no-nonsense approach to protecting your invest-

ments. The process begins and ends with a thorough security vulnerability assessment that is used to pinpoint all vulnerabilities within any particular network. The following are some steps we take to ensure this security for our clients' county courthouse networks.

INTERNAL SECURITY

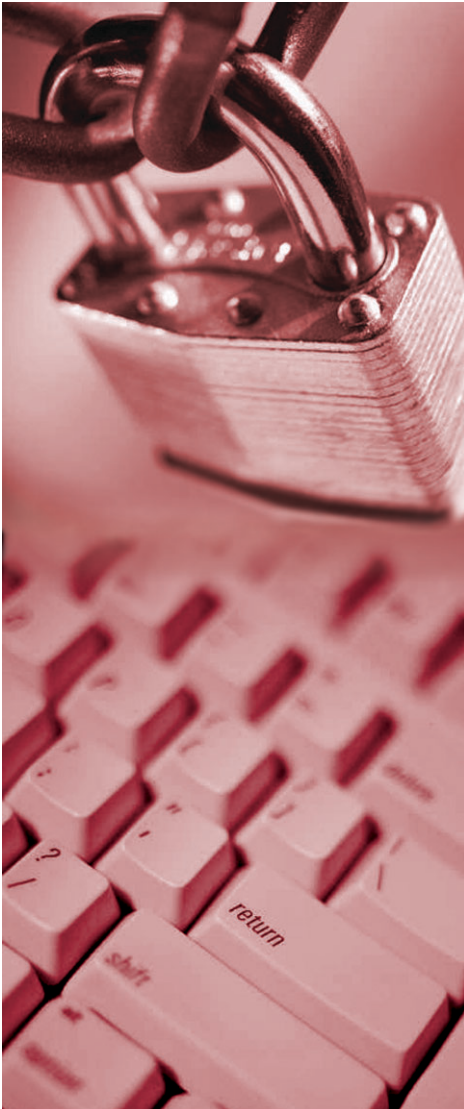
An estimated 70 to 80 percent of all network security breaches originate from within the network. Not always the result of malice, this fact reflects a growing need for multi-faceted network security systems that secure networks from the inside out. Here are some of the steps we take to protect computer networks internally.

AAA Implementation — These measures are known in the business as the "Triple A's" of network security, standing for Authentication, Authorization and Auditing. For a network to be secured, sufficient measures must be taken in all three areas.

Authentication is the method used by computer networks to prove that the person accessing the network is the person he or she says they are. The most common form of authentication is a password, the utilization of which requires its own set of internal policy standards stressing the need for password confidentiality, and the use of strong (alphanumeric) passwords.

Once a person is allowed onto the network, stipulations must be made as to where one can go within the network, how one can get there and how long one can stay. This is called authorization. Through the authorization process, the network can be programmed to allow certain people access to information relating to their position, while refusing information to those on staff who have no reason to view such material. This is most commonly found in permissions assigned to data directories, but can include many other things such as firewall rules, Internet access and email privileges.

To further prove that the above remains true, auditing practices are initiated to finalize the "Triple A" measures of network security. Auditing provides a record, or audit trail, of who connected to the network, what they were connected to, the



Technology Integration of the Modern Courthouse

Being the result of thousands of hours of productivity, data accumulated on a server is truly priceless to any organization.

time that they connected, and how long they were connected, which files were accessed, websites visited, and email sent or received. The audit trail will also record attempted and failed log-in information. Maintaining this audit trail is fundamental to the security of a network.

Implement Content Filtering — A wide-open connection to the Internet via a web browser is like a free-swinging door to the rest of the world. Using a web browser, anyone – either knowingly or unknowingly – can access files, software, music, and most any type of content imaginable, including inappropriate materials such as pornography. While this is part of what makes the Internet such an invaluable tool, it certainly has its trade-offs. The openness of the Internet can lead to the installation of unwanted “SpyWare” software, the accidental reception of a computer virus, and even that unintentional access of inappropriate or objectionable material.

The implementation of content filtering can help to thwart these negative possibilities on your network by blocking access to inappropriate materials and websites. In this process, counties can determine which content and type of Web sites they would like staff members to steer clear from while on the job. Firewall rules are then configured to prevent anyone using a Web browser to access sites containing this content. Content filtering can also target specific “problem sites” that have proven to compromise security, contain inappropriate or questionable material, or to negatively affect productivity in the workplace.

Establish a Data Backup/Contingency Plans — Even with the most air-tight security in place for your county’s computer network, important components can still break down. Sometimes hardware approaching the end of its lifecycle may break down, and other times human error from within the network could lead to a procedural breakdown or data loss can occur due to lightening damage, natural disasters, fire or computer viruses. These are the moments when your network is most vulnerable to a loss of data or, worse yet, a

security breach.

Since no one can tell when and how these failures may occur, the key to limiting your losses and getting your network back up in good working order is to develop a thorough Contingency Plan for these circumstances. A comprehensive understanding of a particular network and its uses is essential in the development of a solid contingency plan. The system engineers at R & D Industries have developed contingency plans for a number of our clients, and we can assist you in planning before disaster strikes.

Contingency plans should be very comprehensive so that it protects your ever changing data. For example, if a new data directory is created, this directory needs to be automatically included in the backup and verification processes. Our backup solutions cover areas including but not limited to: backup device selection, tape backup rotation strategy, personnel policies, tape locations, offsite storage, paper backup logs, data mirroring, server mirroring, server clusters, hardware failover, etc. The bottom line is that we are very particular when it comes to protecting critical data.

Data Backup — Data backup is a standard procedure that should be implemented within all computer networks, regardless of size. Being the result of thousands of hours of productivity, data accumulated on a server is truly priceless to any organization. In the case of a county courthouse, this data also includes gigabytes of critical records that the county is required to safely keep and maintain. The loss of this information would be damaging to any department of the county.

Data loss can take place as a result of a security breach, a virus infection, or simply because of a failed hard drive. Loss of data can take place quickly and unexpectedly, and by the time it is detected, it is too late to worry that your system was backed up properly. That is why it remains critical that a proper backup system is implemented and thoroughly maintained at all times.

“Backup” refers to the process of copying your files to a second source for storage as a precaution in case your computer or network fails. R & D Industries clients

Technology Integration of the Modern Courthouse

benefit from two types of backup security measures. A daily incremental system backs up resaved files on a daily basis. Therefore, any changes made on the network from day to day will be recorded and saved as a backup file. Then on a weekly basis, your entire system will receive a full backup, providing your organization with a means to recover lost files in the event of an unforeseen network emergency.

Implementation of Network

Policies/Procedures — The most robust network security measures available through the application of protective hardware and software can be rendered ineffective without the implementation and enforcement of explicit network user policies, sometimes known as an “Acceptable Use Policy”. These policies should be written and approved with the following goals in mind: increase security, define procedures, outline acceptable use of the network by all employees, and develop a course of action in cases of inappropriate use.

Network policies should include, but will not be limited to, the following documentation:

- Employee Agreement for Computer Usage
- Acceptable Use Policy (For workstation, computer network, & Internet)
- Auditing Policy/Procedures
- Security Incident Plans and Procedures
- Password Policy
- Disaster and Recovery Guidelines
- Laptop Use Policies

Since county networks store Private Healthcare Information (PHI) on their servers, these documented policies and procedures – among others required – must be written and approved in order to comply with HIPAA guidelines. Even on networks that do not store private healthcare information, however, strongly-written policies should always be enforced for the sake of security and department integrity.

EXTERNAL SECURITY

Now that the internal components of your network are secured, time begins to address external security measures that

build another line of defense in the protection of a computer network system. This line of defense is intended to stop infected or questionable content before it even enters a computer network while allowing other information to safely, and sometimes confidentially, pass into the network unscathed.

Firewall Implementation — The implementation of a hardware firewall to your computer network is a necessary move to ensure the integrity of all information coming into your network via the Internet. Set up as your network’s first line of defense for incoming data, a firewall examines each message going into and coming out of a network and blocks those that do not meet specified security criteria.

As the leading Watchguard Firebox reseller in the Midwest, the staff at R & D Industries are experts at utilizing Watchguard’s state-of-the-art firewall technology as a content filtering tool to block either specific Web sites or categories of Web sites by recognizing key words, reducing the risk that malicious content imbedded within Web content could infect your system.

Watchguard Fireboxes also include built-in proxies as an additional protection. The proxies protect against external threats as well as conceal details about the internal network from the public interest. Firebox proxies protect the functions most common to business use of the Internet.

We further create a firewall disposition, and a courthouse policy, which outright blocks file types which are commonly used to propagate viruses. Commonly blocked file types blocked at the firewall level include: .exe, .vbs, .bat, .pif, .lnk, .com, .scr, etc.

The diverse level of security provided by the proper application of a firewall is taken to another level with the implementation of egress filtering. Egress filtering is the solution to a problem caused by two current givens: your exchange server contains private and sometimes confidential information, and some current computer viruses that can infect your exchange server automatically emails random files from the server to unknown Internet recipients. The goal of egress filtering is to expand a firewall’s gatekeeper



Technology Integration of the Modern Courthouse

Besides being annoying and at times offensive, spam also takes up valuable bandwidth and disrupts the normal operations of your mail server, leading to a large loss of productivity.

role to include the scanning of outgoing documents. This can insure that the private information stored on your county's exchange server is protected from leakage into the Internet.

VPN Technologies — A VPN, or Virtual Private Network, is an outside private connection into an existing local area network that can be created for the purpose of safely transferring sensitive or confidential information. The difference between a VPN and other outside network connections is that the connection is made via the public Internet through the implementation of a highly-secure encryption process called tunneling.

So under what circumstances would a county government entity utilize VPN technologies? In the past, counties have contacted the network technicians at R & D Industries to establish VPNs for the secure transfer of private healthcare information in accordance with HIPAA standards. This application has proven to be ideal for department of public health staff members who do much of their work on the road and from their homes.

The application possibilities of utilizing VPN technologies, however, are endless. A VPN can be implemented in special circumstances where a staff member must work from home for a period of time, or even for a department head who puts in extra hours from home in the evening.

Anti-Spam — Spam is simply another name for the junk email most users receive daily – any many times hourly – into their email accounts. Besides being annoying and at times offensive, spam also takes up valuable bandwidth and disrupts the normal operations of your mail server, leading to a large loss of productivity. In the case of offensive Spam, it is the duty of employers to practice due diligence in the elimination of this ugly e-mail. Fortunately, our network technicians have found a solution to spam that at minimum blocks 99 percent of the annoying email.

We use a variety of Spam filtering technologies for our clients, the selection of the best solution is often situation dependent, and depends on how they are connected to the Internet, how their mail

is stored and retrieved, and what firewall and antivirus solution is employed currently.

We most commonly use SpamScreen, which is an add-on product which runs on top of Watchguard firewalls which we implement.

Another solution which we implement is called ModusMail, it eliminates Spam by implementing a multi-level approach using sophisticated internal anti-spam defense tools with advanced POP/IMAP & SMTP security options. This approach accomplishes the following:

- Prevents unauthorized "Open Relay" use of the mail server
- Blocks spammers' scan attacks
- Defends against over 500 multipurpose Internet mail extension (MIME) attacks
- Blocks messages based on Real-Time Blacklists (RBLs)
- Limits number of simultaneous connections
- Allows Blacklists to reject connections from specified addresses or IPs
- Offers reverse DNS lookups using RBL (Reverse Black List) servers
- Supports Whitelists to accept messages from legitimate senders
- Incorporates Bayesian filtering using proprietary SCA engine

ModusMail recognizes 24/7 updates of Sieve filtering scripts and VASC (VOP Anti-Spam Coalition) support to provide clients with yet another layer of Spam protection, all of which is packaged into a professional yet simple-to-use interface.

Of the clients for whom we have implemented ModusMail, auditing records indicate that tens of thousands of spam was eliminated from their inboxes due to the state-of-the-art filtering technology. While you can place a number of the amount of spam messages eliminated, the productivity gained from this elimination is truly priceless for any organization.

Anti-Virus Protection — The addition of virus-checking software to your network will add another layer of protection to your newly-secure network. Integrated use with a firewall will provide you with piece of mind and the assurance that your private documents will be safe from damage, deletion or outside viewing.

Technology Integration of the Modern Courthouse

While spam can become a personal and technical annoyance, a virus can cause much more than disruption within a computer network system. Viruses, worms and Trojan horses, once in your system, can wreak havoc on your organization by modifying and deleting data, damaging the computer system, and taking over its mail server. The disruption can last days if not quickly diagnosed and treated. Therefore, prevention is the best defense for eliminating computer viruses, and there is no better place to implement preventative measures than at an organization's mail server.

While implementing robust antivirus software within your network is a first step toward virus protection, the continual updating of this virus software is the most essential step. New computer viruses are discovered daily, and many have the ability to circulate the globe in a matter of hours. By not updating your virus software daily, your county's network could suddenly be deemed susceptible for a virus when hours earlier it was considered secure.

Because the virus risk always runs high on an unprotected system, our technicians implement virus patterns that automatically update your network daily. By doing this, the potential for human error is avoided, giving your staff one less thing to worry about during a day's work.

Email Technologies

The use of email is required for the day-to-day operation of a county courthouse. Staff members from all departments rely on the application of email technologies to perform such duties as receive legal documents from attorneys, abstractors, engineers, contractors, etc. Without the proper implementation of security measures and enforcement of network use policies, however, the use of email poses a huge risk for any network.

Many of the more common computer viruses are propagated utilizing email. Also, spam poses a risk in productivity, reliability, and liability exposure to a county. (The constant reception of inappropriate or offensive spam in a staff member's inbox could indeed be a heavy liability). Furthermore, improperly configured firewalls or cheap firewalls will allow

anything, including private or confidential documents – which could contain private healthcare information – to be e-mailed anywhere in the world.

The network technicians at R & D Industries, however, have developed a multi-faceted approach that effectively integrates a number of security measures into a single email protection solution. The security measures included in this approach include the following:

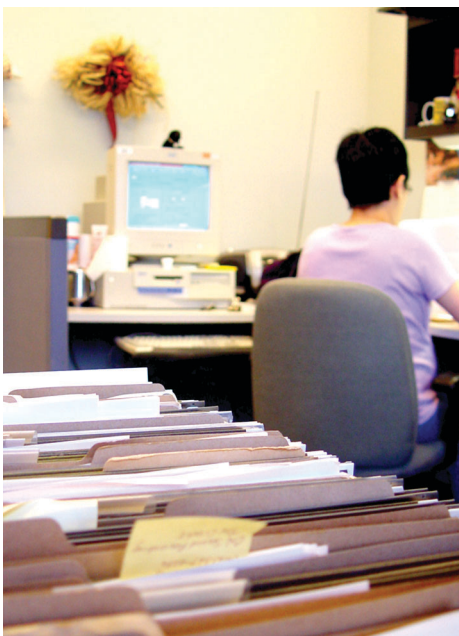
Creating a Firewall Disposition – We create firewall dispositions, and courthouse policy, that blocks file types at the firewall level that are commonly used to propagate viruses. Commonly blocked file types include: .exe, .vbs, .bat, .pif, .lnk, etc.

Anti-Virus Scanning – We have already established why virus scanning and the daily updating of your virus software are essential. Reinforcing this issue only further suggests the importance of this step in the security process, especially when securing your county's emailing activities.

Implement Anti-Spam Technologies – The anti-spam technologies that we use include, but are not limited to, using Reverse Blacklist (RBL) servers; protocol filters which can block specific subjects, topics, senders, etc.; global whitelists and blacklists; and Bayesian Filtering. Bayesian Filtering scans the content of your incoming emails and, using a series of strong indicators that identify spam content, either identifies the email as spam or legitimate mail. Our spam solutions work, and work very well.

Disclaimers – We can program your email system to include common disclaimers that are attached onto the end of all outgoing messages. Much like disclaimers on a faxed document, these would outline all intentions and purposes for your outgoing emails and outline steps to take if one receives a document from your county network in error.

Implement Email Archiving – At the government level, precedent suggests that all incoming and outgoing email is a matter of public record. Therefore, it is essential that the email sent and received within any county network is securely archived. This also remains essential in maintaining solid documentation of actions taken within your network in case it is someday



Technology Integration of the Modern Courthouse

needed for personnel or legal issues.

Document Imaging

Document imaging has quickly become a universally accepted system for filing records. The basis of the system is the conversion of hard copy files to digital files which can be accessed from your network, and anywhere in the world via the Internet. For businesses, corporations, government offices, schools, and any other organization with years of accumulated records, this means greater efficiency through the system's use of simple scanning and indexing processes, effortless accessibility, and reliable, long-term storage.

The process of creating digital documentation is intended to prevent organizations from becoming bogged down by using paper as their primary "media." As any official or business professional can attest, paper records can quickly stack up, creating a challenge for the organization in securing the future access of these documents. R & D Industries offers document imaging solutions which will remove these barriers and create new-found efficiency within your organization.

A basic document imaging system is made of five components:

Scanning: Great scanning and Optical Character Recognition (OCR) technology advancements make paper document conversion into a Group-IV TIFF file cheaper, easier and faster.

Storage: The records storage system provides reliable long-term record retention. A good records storage system will accommodate changing documents, growing volumes and advancing imaging technology.

Indexing: The index system creates an organized document filing systems and makes future retrieval simple and efficient. A good indexing system will raise the effectiveness of existing procedures and document filing systems.

Retrieval: The retrieval system uses information about the documents, including index and text, to find images stored in the system. A good retrieval system is intuitive and makes finding the right documents fast and easy.

Access: Document viewing should be readily available to those who need it, with the flexibility to control access to your records. A good access system will make documents viewable to authorized personnel only, whether in the office or over the Internet.

Beyond the basics, a solid document imaging system must also address network security, backup procedures, document audit trails and "forklift upgrades", a procedure describing the need to upgrade the data and its system every few years. Addressing these prevention and maintenance issues will ensure the safety and accessibility of your digital documents for years to come.

Audio/Visual Systems

County government offices that have chosen R & D Industries for their computer network services have at times asked more from us within the realm of audio/visual systems, and we have accommodated. Having been in the audio and visual business for 20 years, R & D Industries maintains an A/V engineering division that has worked with countless clients, including government offices, in the development of audio/visual systems for a number of purposes, including acoustical analysis and room treatment in courtrooms, A/V system design for boardrooms, intercom systems, etc..

Whether they are designed to enhance presentation capabilities in a board room or to improve communication and hearing in a courtroom, our A/V systems are designed with our clients' specific needs in mind. Our systems can be designed as basic systems that feature a digital projector and screen, or a more complex scheme that integrates a projector, interactive whiteboard, overhead and/or document camera, and a sound reinforcement system into one easy-to-use system.

The process of creating digital documentation is intended to prevent organizations from becoming bogged down by using paper as their primary "media".