

WHITE PAPER.

Security and Integrated Justice Information Systems.

Sunil Misra, Chief Security Adviser & Managing Partner
Unisys Global Security

Paul Stamp, Unisys Security Architect

Justice organizations are integrating systems and sharing information. Increased connectivity means greater threats to information security. Are you taking the necessary steps to protect sensitive data?

- > Consulting.
- > Systems Integration.
- > Outsourcing.
- > Infrastructure.
- > Server Technology.

UNISYS

Imagine it • Done •

If a recent audit of U.S. federal agencies is an accurate barometer, the public sector has a long way to go in securing its computer systems and data. Despite years of legislation and guidelines—and in an environment of heightened security concerns in the post-9/11 era—federal agencies still fare poorly in ratings by the General Accounting Office (GAO), which has been auditing information security since 1996. According to the GAO's latest report card, 14 of the 24 agencies tracked brought home a failing grade, while the highest score, only a B-minus, was garnered by the Social Security Administration.

The good news is that government security officials are making clear progress, actively developing and implementing comprehensive security measures. But there is much work to be done, as the threats continue to proliferate and the complexity of government systems increases.

Nowhere is this more true, perhaps, than in criminal justice. Police departments, court systems, and corrections facilities are relying on information systems to an unprecedented degree. And as justice organizations work to further integrate systems and better share information, those systems and data repositories become more complex—and more difficult to manage and protect. Just as significant, justice is increasingly sharing information with non-justice entities—information that is highly sensitive and must be carefully guarded to ensure privacy and prevent misuse.

It's clear that information security is of paramount importance to justice—and that justice organizations must take active steps to make information security a priority. To this end, justice organizations must ask themselves hard questions and consider a broad range of issues to ensure the confidentiality, integrity, and availability of information. They must evaluate these issues from both the tactical, short-term perspective and strategic, long-term viewpoint.

Finally, justice organizations must establish and implement an overarching security policy. Such a policy delineates the technologies, processes, and behaviors that protect data and promote an environment of trust; provides a stable yet flexible security foundation that responds to changing technology and security needs; and establishes information security as a core function that enables enhanced systems integration and increased information sharing both within and beyond the justice community.

The need for integration.

For justice organizations, a primary driver of information security is the growing need to share information. Such information sharing can help justice fight crime, ensure public safety, and maintain accurate and up-to-date information about offenders in the justice system. Because such information often resides in disparate databases scattered throughout city, county, state, federal, and even international organizations, the need to integrate systems, in some fashion, is paramount.

Integration of justice information systems does not imply that all information is shared at all times. Instead, agencies share key information at primary decision points throughout the justice process. Such integration can be enabled by a number of technologies and approaches, including consolidated information systems, data warehouses, middleware applications, document sharing, and network and Internet connections. To be effective, integration must take place horizontally—among first responders, investigators, courts and corrections—and it must take place vertically—across city, county, state, tribal, national, and international boundaries.

In fact, nearly every state in the union is planning or implementing integrated justice information systems. The agencies that can be involved in an integration project vary widely and can include the state bureau of investigation, attorney general's office, department of corrections, juvenile justice authority, highway patrol, and department of revenue—plus the Federal Bureau of Investigations (FBI) as well as local law enforcement agencies, prosecutors, and courts. Information sharing might also extend to health and human services organizations, treatment services providers, educational institutions, and licensing authorities.

The potential benefits of integrated justice information systems are significant: access to more accurate and timely information, a higher quality of justice, reduced redundancies in data entry, decreased costs for data storage, streamlined and more cost-effective processes. But before they can reap these benefits, justice organizations must grapple with a range of challenges—including security.

A growing threat.

According to a recent survey by the Computer Security Institute, 9 out of 10 large U.S. companies and government agencies detected a computer security breach in the past 12 months. More than one security expert has called 2003, "the worst year ever" for security breaches—until January 2004, when the Internet was hit with MyDoom, the fastest spreading worm in history. Such security violations carry an increasingly large price tag. The average cost of a MyDoom-type virus to a large business is \$1 million in system cleanup and restoration, reports research firm TruSecure.

In the public sector, federal agencies are the most likely to be attacked; the Department of Defense deals with hundreds of hack attempts every day. But there is growing concern for lower-profile points of attack such as local governments. Cyber-terrorism is among the top three worries for municipal governments, according to a recent survey of 725 cities by the National League of Cities. Yet only 26 percent of U.S. cities have developed strategies to address these attacks.

For justice, in particular, security is an escalating issue, because justice relies more heavily on information systems and increasingly integrates those systems across agencies. Although justice organizations have been using computers to capture and manage information for decades, until recently these information systems were the electronic equivalent of file cabinets. The data was kept under lock and key, and the owner of the data was responsible for gathering, managing, and sharing it.

Today, more sophisticated information systems enable users to create customized, multidimensional information repositories, access data and applications from virtually any location on a variety of devices, and share that information in complex ways with a broad range of users. Issues such as where data actually resides have taken a back seat to questions of who can access the information and how information can be combined, shared, and reused among a growing community of users.

The complexity of sharing justice information—and the vulnerability of that data—is exacerbated by the proliferation of the Internet. As an inexpensive and user-friendly technology, the Internet has emerged as a primary means of sharing information among justice organizations and making limited amounts of justice information available to the public. In addition, states are using Web-based systems to disseminate criminal information to users such as school districts and court officers.

But as much as the Internet is a valuable tool that can dramatically facilitate information sharing, it introduces a new range of security threats. As a vastly interconnected system, the Internet increases exponentially the potential sources of attack. From viruses and worms that can bring down systems, to hacker attacks that can compromise data, to denial-of-service attacks that can lead to legal liabilities for unaware victims, the Internet introduces a range of threats that make it far from a safe environment.

What's more, as justice organizations further rely on information systems and information sharing, the value of that information increases. So too does the cost to protect it—and, in particular, the financial repercussions should that information or the systems it resides on be compromised. From tangible matters such as expenses for restoring damaged systems and information, to difficult-to-measure issues such as the financial impact of lost productivity, to intangible aspects such as a loss of public trust, the price tag for a security breach can be large indeed.

In an era of increased public scrutiny and demands for greater accountability among organizations both public and private, security and its associated costs are no trifling matter. And, in an age of terrorist acts and Orange Alerts, there are new, international, and more pervasive threats than ever before.

Unique challenges.

Electronic communication is occurring more frequently and is involving a broader range of information. The points of interaction among internal systems, external organizations, government employees, and the public are increasing. The result is a dramatic rise in potential points of failure—and a measurable increase in the number of security breaches. In 2002, 82,094 security incidents were reported to Carnegie Mellon's Computer Emergency Response Team (CERT)—a number that increased to 137,529 in 2003.

But several issues are unique to justice information systems, and these factors complicate integration—and security—efforts. For starters, as justice agencies share information across organizational boundaries, they must keep in mind that not all information can be made available to every party or at every transaction point. Although information sharing is integral to integrated justice, the risks involved in sharing all justice information, much of which is highly sensitive, are simply too great. Consequently, selective and secure information sharing is essential.

In addition, justice systems must comply with rigorous legal and regulatory requirements—requirements that can vary from one level of government to another. Likewise, the information maintained in justice systems must meet stringent requirements for integrity if it is to be used in court procedures and legal processes. That imposes distinct requirements for technologies that ensure electronic integrity and trust.

What's more, justice must increasingly communicate with the public. Such communication can be one-sided, such as posting lists of criminal offenders to the Internet. Or it can be far more complex, as with electronic case filing systems that allow members of the legal community to use the Internet to file court documents.

This electronic communication presents a range of security needs. In the first example, the public must trust that justice information posted online is authentic. In many cases, the agency that posts the information is legally responsible for ensuring that the information is accurate. In the second example, legal documents transmitted to the courts must be protected against exposure to unauthorized individuals. In addition, the parties at both ends of the transaction must have assurance that the documents originated from the claimed source and weren't tampered with during transmission.

Just as important, as justice organizations replace paper-based activities with electronic processes, it's increasingly important that systems remain available so that justice operations don't grind to a halt. Just as businesses in the private sector can no longer operate without information technology, so is justice increasingly dependent on technology and interconnected systems.

Finally, there's one aspect of integrated justice information systems that doesn't directly involve security—but that security can help address. While part of the same justice process, police, courts, and corrections are focused on different aspects of justice and can sometimes work at cross-purposes. Any integration initiative must take into account the political realities of interagency communication. Effective security can help build trust that leads to truly effective integration and information sharing.

Balancing need against risk.

It's clear that justice organizations face a distinct need to integrate systems and share information. It's also clear that they must grapple with unique and growing risks to their systems and data. These facts point to a fundamental challenge in managing information.

If justice organizations keep their information systems behind lock and key, those systems remain safe. Yet by doing so, they can make it difficult to achieve their strategic objectives—or to achieve adequate returns on their information technology investments. On the other hand, if justice organizations open up information systems and share data within and across organizational boundaries—without implementing the appropriate security measures—those information assets become vulnerable.

What's needed is for justice organizations to take a proactive approach to balancing the requirement to share information with the security risks inherent in doing so. This balanced view is a fundamental and, for many justice agencies, new approach to security. Seen from this perspective, security is less about building a fence around information assets and more about managing risk and enabling new processes.

To achieve this balance between need and risk, justice organizations must ask themselves rudimentary questions about the information they manage, the processes they need to enable, and the security measures they must embrace. And to attain an appropriate and effective level of security, justice organizations must examine tactical, short-term concerns and strategic, long-term issues.

A tactical approach: immediate needs and threats.

In the short-term, justice organizations must respond to immediate security threats. Doing so begins with an understanding of three primary aspects of security: confidentiality, integrity, and availability. Confidentiality deals with the mechanisms that support information access policies, ensuring that information isn't exposed to unauthorized use. Integrity concerns the accuracy of information and requires technologies and processes to keep information from being tampered with. Availability ensures that information systems are available when needed. This is particularly important for justice systems, which can affect the safety of civil servants and citizens.

A complete approach to security addresses confidentiality, integrity, and availability through a security architecture that includes technological, procedural, and physical safeguards. The objective should be to protect information from accidental or intentional modification, destruction, or disclosure, and to support the integration of justice systems. This enables the sharing of trusted information and ensures the continuity of justice organizations.

The goal, then, is to engender an environment of trust among justice organizations and between justice and the public. Electronic trust will thrive if each organization can be confident that all parties with access to shared information conform to a baseline of practices to safeguard that information. This environment of trust is a prerequisite to realizing objectives for sharing justice information, enhancing justice processes, and improving public safety. To this end, a tactical approach to security involves several key issues, including authentication, data security, identity management, and privacy.

Authentication and access control.

Authentication and access control are a first line of defense. They ensure that individuals who want to access a system are who they claim to be, and are acting within the confines of the access privileges they have been granted. Authentication technologies can be organized by three factors: something you know, something you have and something about you. A password or PIN is something you know. A smart card is something you have. While biometric mechanisms, such as a fingerprint or iris pattern, are something about you. A highly secure system may involve multiple authentication factors—for example, combining a password with a smart card.

Data security.

Data security provides detailed information control and supports need-to-know policies. In integrated justice situations, multiple organizations may require access to subsets of information stored in a single database, or pieces of data scattered across multiple databases. It's important to maintain separate data views for each user group, so that users can access the information they need while being restricted from information they are unauthorized to see. Such role-based security ensures both confidentiality and availability, making information available to those who need it while protecting sensitive data from those who don't.

Identity management.

Identity management essentially combines authentication and database security to provide rigorous security while ensuring streamlined processes. Increasingly, users demand real-time access to information at any time and from any location. At the same time, government regulations require tighter controls for information access to protect privacy and enhance accountability. Meanwhile, HR and security managers must manage employee turnover, staff reorganizations, and changing user roles. Delays in granting access to systems and information impede justice processes. Delays in changing access privileges introduce risks of security breaches.

An effective identity and access management solution can help justice organizations meet these challenges. Directory services can consolidate or synchronize identity information dispersed throughout the agency. Automated provisioning and deprovisioning can enhance productivity and security. Authentication and access control solutions can reduce the number of discrete sign-ons while providing the appropriate level of security and access to systems and information.

Identity management is increasingly important to justice organizations. It isn't uncommon for an integrated justice information system to involve thousands of diverse users, ranging from small agencies with just a few standalone PCs, to midsize and large agencies with a local-area network consisting of both justice and non-justice users, to mobile users who access the system from remote locations over dial-up connections.

What's more, the justice community is dynamic, as personnel are transferred or promoted and new officials are appointed or elected. In the event of a crisis, a new set of users may require access to certain information, while another set may be restricted from seeing sensitive data. Each involves an associated change in roles and access privileges. Identity management provides an effective way of responding to these shifting needs.

Privacy protection.

Privacy has emerged as a key public concern. Citizens expect that personal information will remain protected, and they assume that automated processes such as online licensing are secure. They will surely demand accountability if justice information is tampered with or accessed by unauthorized individuals.

While security is about protecting information from accidental or intentional alteration, destruction, or disclosure, privacy is about controlling who is authorized to access information and the right of individuals to keep information about themselves from being disclosed. It is possible to secure information without making it private, but it is not possible to protect privacy without security.

Privacy standards for criminal history information have long been governed by statute and regulation. All states have adopted standards to ensure the completeness and accuracy of criminal history information, and all have enacted laws or regulations setting standards for the use and dissemination of criminal history information.

But new developments may be rendering old privacy safeguards obsolete. These developments include dramatic improvements in information, communications, and identification technologies, accelerating initiatives to integrate justice information systems and an increasing interest in sharing justice information with non-justice entities. It's no surprise, then, that in recent years Congress has considered or enacted privacy legislation that applies to telecommunications, online data repositories, tax records, credit reporting, motor vehicle and license information, medical records, and child privacy. State legislatures, for their part, have considered hundreds of privacy bills and enacted dozens of privacy statutes.

A strategic approach: preparing for the future.

While it is important to address short-term issues, security is never static, and a long-term, more strategic perspective is imperative. For starters, new technologies introduce new security concerns. From intranets to extranets to public Web sites, from remote access to e-mail to personal digital assistants (PDA), there's a seemingly endless progression of technology developments, each with unique security requirements.

What's more, new processes introduce new risks. A police station might appear to be a secure environment. But if the stationhouse is integrated with the department of motor vehicles, and the department of motor vehicles allows license renewals through a public kiosk, the police station becomes vulnerable to new attacks. And the attacks are certainly constant. From stolen laptops to network intrusions, from worms to viruses—there are now more than 70,000 computer viruses in circulation—the assault on information systems is endless.

Likewise, the needs of the justice community are increasingly dynamic. As justice organizations share information with a broader range of user groups—including non-justice entities such as health and human services, schools and higher education, and licensing authorities—their security requirements change and grow. In addition to calling for additional protection, integration requires that each organization meet the regulations and certifications that apply to all participants in the electronic community. In an age of potential cyber-terrorism, the number of regulations and certifications will only increase, especially as justice organizations share information with new partners, including federal agencies such as the U.S. Customs and Border Protection and international organizations such as Interpol.

What's needed is a flexible and adaptive security architecture that can meet agency needs both today and in the future. Such an architecture must enable justice organizations to allow or restrict access to systems and information in real-time, adapt quickly and effectively to new regulations and certifications, and enable safe integration that supports new and more effective strategies and processes.

Moving toward a solution: security policy.

Protecting information requires a range of technology solutions, including technology that enables justice organizations to identify the specific user, identify the specific device being used, protect data transmissions over the network, protect systems and databases from unauthorized users, and monitor for unauthorized intrusion. But technology is merely a means of implementing security strategy. Fundamentally, security must combine technology, operations, and organization.

To that end, justice organizations must develop and implement an overarching security policy that dictates how security will support justice processes. Security standards, technologies, procedures, and behaviors then become ways of carrying out that policy. It's the difference between piecemeal fixes that address specific security problems and a holistic approach to security that ensures the proper balance between access and risk.

An effective security policy unifies all aspects of security measures into a single strategy. It specifies the value of various information assets, the level of risk for those assets, and the technologies and procedures that will protect them. It also deals with specifics such as how personnel authenticate themselves, how often they must change passwords, who authorizes access to systems, and how authorization levels are granted.

To be manageable and cost-effective, a security policy must also be repeatable. Ultimately, a security policy establishes a set of standards—for operating environment, for how justice records are stored, for how justice systems are integrated, and so on. Once those standards are established, they can be applied consistently and cost-effectively.

Security policy involves several key issues, including assessment, technology, automation, procedures, physical security, training, a response plan, testing and evaluation, and organization.

- ▶ **Assessment**—Addressing security begins with a thorough assessment of vulnerabilities, the risk of a security breach and the impact a security incident would have on justice processes. Justice agencies must assess how they organize data, how they determine which data must be protected, who is responsible for that data, and who can access that data. In a typical scenario, an assessment of this type might reveal dozens of vulnerabilities. The next step is to evaluate and prioritize those vulnerabilities according to regulatory impact or their affect on justice operations. Finally, look for security technology weaknesses, security process weaknesses, processes that can be easily circumvented, and processes that are simply not being executed.
- ▶ **Technology**—Although security technology is only one aspect of a security policy, it is an important aspect. The policy should specify the technologies and associated procedures that will protect the environment. Such technologies will likely include antivirus software, firewalls, intrusion detection, and data backup systems, as well as the practices to ensure those technologies are used effectively.
- ▶ **Automation**—Technology can also help by automating security processes. For example, provisioning solutions address operational challenges such as how long personnel and constituents have to wait for access to systems or facilities, or how many user accounts are left open and for how long after an employee has left. A provisioning solution can automate processes to enhance their efficiency and provide consistent enforcement of policy. This can include provisioning of logical and physical information assets to new users, managing user privileges as organizational relationships change, and revoking access rights and recovering information assets when information sharing is no longer necessary.
- ▶ **Procedures**—There are a broad range of procedures and user behaviors that can have a profound impact on security efforts. For example, as personnel change roles, they may require greater access to systems and information. They may therefore have opportunity to cause greater harm, even inadvertently, by accessing or making available information. In addition to strict rules for granting access privileges, justice organizations should consider policies about background screening, such as state and federal fingerprint-based records checks, and re-investigations before granting a higher level of access. Justice organizations also need to consider penalties for violations of access policies, especially if such a violation results in disclosure of sensitive information to unauthorized individuals. Such a policy should address activities that result in unauthorized alteration or destruction of information, system downtime, or theft of computer media such as memory chips, data storage media, or even hardcopy printouts. Criteria for disciplinary action may be based on local or state statues and should take into consideration the extent of loss or injury.

Finally, all parties involved in information sharing should have written and signed agreements that specify a baseline level of security. Such an agreement might extend to non-justice agencies and visitors to physical sites.

- ▶ Physical security—Although often overlooked, physical security is a key part of information security. From securing data centers to protecting laptops, security must take into account traditional physical security components involving people and property. Although physical and information security have traditionally involved distinct organizations, procedures and budgets, they can no longer operate independently.
- ▶ Training—Training and certification can ensure that users who access systems and information understand how they operate and have the appropriate level of training. Although training may specifically target security personnel, all users should view security as their responsibility and behave accordingly. Justice organizations should establish and disseminate rules for e-mail usage, Web access, and related activities.
- ▶ Response plan—An effective security policy includes guidelines for a response after a security violation has taken place. It should identify the personnel who will respond and what their responsibilities will be. It should also establish procedures for determining the severity of the breach and the appropriate response. The response plan should also address communication activities. In the event of a security breach, justice agencies may need to inform local law enforcement, federal agencies such as the FBI, and response organizations such as CERT.
- ▶ Testing and evaluation—No security policy is complete without provisions for testing and evaluation. Justice organizations should conduct audits to ensure that security policy is being implemented and security measures are at the proper levels. They should also conduct regular "fire drills" to determine whether they are prepared to respond in the event of a security violation.
- ▶ Organization—Finally, experts agree that it is essential to have a clearly defined governance structure for security. Justice organizations must establish ownership and responsibility for data and processes—and, even more important, ownership and responsibility for security strategy and policy. It is probably wise to set up an executive board for management oversight, planning, and coordination, with appropriate subcommittees to address issues such as technology and personnel policies. Also ensure there is continued support from executive management and stakeholders in each participating organization. Such governance is particularly important in widely distributed organizations such as law enforcement.

Help when you need it.

Security policy and standards are integral to justice agencies and best accomplished by justice executives, committees, and personnel. But few justice organizations have the security expertise or staff to effectively develop and implement all aspects of an effective security architecture. As a result, justice organizations should consider whether and when they should turn to an external services provider for help.

From assessing risks to deploying security technology, from managing specific security processes to providing turnkey, outsourced security services, a security services provider can ensure appropriate, cost-effective security. Qualified security services providers have in-depth knowledge of security issues and technologies, and they have invested in the staff and training necessary to remain current with security issues. They also have experience applying security to a variety of environments, and the proven methodologies that make security manageable and cost-effective.

Look for a security services provider that can offer proven expertise and extensive experience in advising, transforming, and managing security solutions for corporations and government organizations around the world. Security competencies and capabilities should extend from strategy and consulting services, to implementation services, to network and physical security services, to the delivery of identity and access management solutions. The security services provider should demonstrate a multidimensional understanding of security issues, enabling it to take a holistic approach to assessing vulnerabilities and deploying corrective measures. Finally, it should become a trusted partner, working with the justice agency over the long term to develop, implement, and manage a comprehensive security solution that meets the agency's unique needs.

Throughout the criminal justice community, there is a growing reliance on information systems. There's also an increased focus on integrating systems and sharing information among both justice and non-justice entities. These factors place new requirements on how justice organizations ensure the confidentiality, integrity, and availability of sensitive information.

By carefully balancing the need to share information against the risks of doing so—and by fully considering both short-term, tactical factors and long-term, strategic issues—justice organizations can adopt a comprehensive, holistic approach to protecting their information assets. The result will be effective security that protects systems and information while streamlining justice operations and enabling more effective processes that ensure public safety, deliver new services to constituencies and improve the quality of justice.

A security checklist.

Justice organizations must strike a balance between the need to share information and the risks inherent in making information available. To do so, they should consider the following steps:

- Identify need—Determine your need to integrate systems or share information both within and beyond organizational boundaries.
- Assess risk—Identify the level of vulnerability for systems and information, and the consequences should a security breach occur.
- Balance need and risk—There is no perfect security. Determine how you can best make information available while protecting it from unauthorized use.
- Address immediate threats—Deploy short-term solutions to ensure the confidentiality, integrity, and availability of information.
- Consider long-term strategies—Ensure that your security architecture is flexible and adaptive to changing technologies and security requirements.
- Create a policy—Unify all aspects of your security measures in an overarching policy that specifies standards, technologies, procedures, training, testing, and a clearly defined organization that will ensure the protection of justice information.

Notes

Notes

For further information, visit www.unisys.com

Specifications are subject to change without notice.

© 2004 Unisys Corporation
All rights reserved.

Unisys is a registered trademark of Unisys Corporation.
All other brands and products registered herein are
acknowledged to be trademarks or registered trademarks
of their respective holders.

Printed in U S America 3/04



4136 4209-000