IBM Global Services

IT Security.

Creating value with comprehensive security solutions for public safety and justice agencies

Key Topics

Addresses the need for e-business solutions within law enforcement and criminal justice agencies

Defines the most frequent threats to sensitive data, which come from internal rather than external sources

Clarifies common misperceptions surrounding information systems security

Identifies proven strategies for securing information technology assets

Presents a comprehensive approach to IT security to help organizations develop best-practice policies and procedures

Discusses emerging technologies that can enhance and improve security measures

Summary

Regardless of the need for, and the availability of, technology and funding, many law enforcement and criminal justice organizations are reluctant to pursue the opportunities presented by e-business and other information technologies (IT) to transform and streamline internal operations. This is often due to the belief that replacing or supplementing standalone mainframe systems with networked computers and implementing automated reports and computer networks will expose them to attacks by computer hackers.

While use of networks can increase exposure to attacks on information systems, assets and databases, the main source of security threats resides within an organization. This paper discusses IT security with the intention of putting these threats into realistic perspective by identifying the areas that represent the most frequent threats, and providing seven basic strategies for planning IT security so that your agency's information, communications and e-business assets are protected.

Identifying a strategic opportunity

Many organizations are hesitant to implement new technology solutions, such as e-business, due to the fear of becoming vulnerable to network attacks that could compromise critical information. Part of the problem lies in the misconception that planning and implementing adequate IT security measures—conducted with a view toward protecting an entire system against attacks—results in prohibitive costs. These perceived costs, combined with the damage that could result from the loss of extremely sensitive information, make the concept of networking seem unreasonable, regardless of potential gains to be achieved from today's technology solutions.

Moreover, while improperly implemented IT networks can increase exposure to security breaches on information systems, outside attacks are rarely the biggest threat. Rather, most threats to sensitive data come from trusted sources within an organization. This real danger is often created by the absence of even minimal attention to planning and implementing basic IT security measures.

The reality is that law enforcement and criminal justice agencies have an unprecedented opportunity to use IT to transform operations and collectively provide better service. Advances in technology can be applied directly to the core business activities of law enforcement and justice organizations. With the increasing affordability of technology and the availability of funding from the federal government, IT upgrades are swiftly becoming a reality.

Overall, the primary threats to information security are a lack of thorough security planning, an absence of established policies, ineffective training and insufficient monitoring of personnel activity. Planning, based on a realistic assessment of needs and risks, followed by meaningful implementation of a best-practice plan, can provide effective and cost-efficient protection against the vast majority of today's security threats.

Perception versus facts

If one were to analyze the amount of money budgeted and spent for criminal justice IT, the results would show that many organizations have made the commitment to meet new IT challenges. Yet there has also been an increase in the number of reports of information systems being attacked and penetrated by hackers, in addition to rising reports of illegal use of justice database information, and thefts of critical data and IT assets.

The increasing frequency of these reports has discouraged many agencies from venturing beyond their existing closed systems. However, new business requirements imposed on criminal justice agencies demand that they change the methods by which they acquire, share and disseminate information. These changes have occurred due to:

- Community and problem-solving policing policies, with their fundamental need for IT support to collect and share information

- Recognition that line personnel need to spend more time on their primary responsibilities and less time on completing reports

- Increased use of integrated justice models to improve the quality and reduce the operating costs of criminal justice

- Expanded legislative mandates in the United States—both federal and local—that impose additional reporting requirements on law enforcement and criminal justice agencies (e.g., Megan's Law, Brady Bill, mandatory sentencing)

- Augmented use of criminal history for noncriminal purposes, such as approval for certain types of employment or public housing.

Weighing e-business solution options

In the dynamic world of e-business, change has become a necessity, not an option. Yet some agencies have responded by implementing standalone systems that provide new services but are not integrated with, or complementary to, the organization's legacy systems, thereby increasing the complexity and costs of supporting IT.

Fear of attack, threat of compromise of information systems and lack of confidence in the ability to provide adequate security are major reasons for avoiding electronic exchange of information and sharing of services. However, there is still a growing need to implement more effective solutions for managing and distributing data to accomplish the following:

- Streamline work processes
- Disseminate data beyond organizational boundaries
- Distribute information systems to the field
- Exchange information with multiple outside agencies and individuals.

Protecting data from internal threats

Perception of the problem is actually worse than the reality. Highly publicized hacking incidents and movies like *The Net,* which showcase major police systems being routinely penetrated, promote and perpetuate the perception that outside sources pose the most critical threat to information systems. In fact, internal threats from sources within a trusted domain cause more damage than outside intruders. For example:

- An entire department's network was brought down by a virus that was passed by diskettes distributed from the department's planning division to collect survey information.
- The chief of intelligence overseeing a hierarchical intelligence system had his user ID and password displayed on his monitor with detailed login instructions.
- A senior police department official sold a file containing the description and license plate information of all undercover cars to organized crime.
- A novice network administrator of a midsize police department gave administrator privileges to every user, thus giving all users access to each other's information and passwords.
- Application programmers at a major police department were allowed to put new—and unknowingly compromised—program code directly into production without review, which brought the entire system down for 24 hours.
- A state set up a Web site with no firewalls. Within 24 hours, its user ID and password file was posted at a hacker conference.

None of these stories involved a hacker successfully attacking an agency information system—all of these incidents could have been prevented by some basic planning and training. While there is increased risk of external attack as a result of new technologies, it is a proportional threat that can be abated.

Trends that have led to increased IT security risks

Causes of increased exposure to information security threats vary. However, sweeping changes in the way IT is applied in justice agencies are creating a fundamental need to alter the way information security is planned, implemented and managed. Among these basic trends are:

- New business models in which the public sector mirrors private sector IT use

- Dramatic increase in the growth of IT as computers and networks become intrinsic to various parts of the everyday operation of justice agencies

- Affordability of technology in which basic IT costs are lower than ever, and the cost of new technology is dropping rapidly due to advances and increased competition.

Like almost every business challenge, these trends provide opportunity for improvement of IT security practices, along with the issues they create.

Creating a new business model

Community and problem-solving policing strategies, state-of-the-art integrated justice initiatives, and advanced systems for measuring and managing corrections programs are all examples of business innovations in the justice environment. These innovative business models often involve a transition from a centralized, closed information management model to a distributed, open-networked architecture, with information and physical assets widely distributed across the entire justice "enterprise."

This transition can present complications, such as difficulty in protecting assets, monitoring operations and responding to problems, since there are more points of potential exposure. Yet the benefit of IT simply cannot be ignored because these challenges are present. Significant productivity enhancements can be gained by the proper application of IT to improve inefficient, paper-intensive business processes. Often, legislation or other legal activity requires agencies to implement new IT. More importantly, though, implementing e-business solutions to streamline data management and distribution can improve access to critical, lifesaving information. Authorized users with timely access to information on criminals and crime can make safer and more informed choices.

Remarkable growth in the use of IT

Computers and networks are an integral part of our lives. Regardless of the extent of use, IT is often taken for granted. Computers, networks, the Internet, intranets and extranets can provide a conduit for fraud, theft and dissemination of illegal information and materials. New kinds of crime are devised and old schemes are given new life.

However, this growth has also driven advances in technology, emergence of standards and identification of best practices. As pioneers made mistakes, and the lessons learned improved the technology, we all benefited. Security practices have improved as a result of challenges and high-profile security breaches, and solid, best-practice models have emerged.

Decreasing costs of IT

Regardless of the metric used, basic IT and new technology costs continue to decrease. As a result of this, nearly all organizations today can afford a computer, thus increasing the population at risk and the number of potential IT abusers. However, decreasing real costs applies to core justice business systems and to security systems. Additionally, because the private sector has laid the groundwork, many new hardware and software products now have built-in security features at no additional cost.

IT budgets in the public sector have increased more than at any time since the late sixties and early seventies. Federal crime bills (e.g., COPS MORE) are providing billions of dollars for the express purpose of upgrading or replacing public sector information systems.

Comprehensive planning, security and threat assessment

Many organizations have resisted investing in e-business solutions because of the persistent and exaggerated belief that hackers and intruders will immediately besiege them. However, new business models, new IT applications and the decreasing cost of technology are driving justice agencies to adopt e-business applications. How then, can the justice agency plan for adequate information security?

The science fiction book *Hitchhikers Guide to the Galaxy* has a rule for dealing with challenges: Don't panic.[1] This is good advice for IT security planning, too. Despite increased exposure to potential intruders, the experience and tools to build effective defenses are already available and constantly improving. With effective, advance planning, it is possible to respond rapidly and appropriately to security threats.

Overall, IT planning must be comprehensive, flowing directly from an organization's operational plans. In addition, an effective plan must describe the business requirements that map to operational goals. There are many ways to meet IT requirements, and substantial cost differences, but there should always be a clear justification for every dollar spent, and security must be built in to the IT infrastructure from the beginning.

Seven strategies for planning IT security

Data in an IT system is at risk from various sources—user errors and malicious or non-malicious attacks. Establishing an effective set of security policies and procedures to reduce risk requires the use of comprehensive, best-practice strategies.

Seven strategies for IT security	Benefits
Simplify your security	• Increases the likelihood that procedures will be followed • Keeps costs down
Develop policies, procedures and penalties	• Provides an effective plan of action for addressing security breaches
Provide system training	• Increases awareness of personnel • Improves understanding of critical security issues
Use available security products	• Provides products that have been tested and proven • Includes comprehensive user documentation
Compartmentalize information, assets and users	• Improves inventory management • Provides configuration control • Enables problem reporting • Manages supplies and sales • Documents and manages system requirements
Establish realistic security administration goals	• Enables more efficient allocation of resources
Regularly test, audit, inspect and investigate sites	• Ensures that security failures are addressed prior to an attack

Keep your security—and your applications—simple

As with any information system, when a security solution is too complicated, users will avoid or circumvent it, thus defeating its purpose. If users are unwilling to abide by an overly complicated security system, its usefulness is drastically reduced. Additionally, when application systems are made needlessly complex, regardless of how tightly integrated they are, they offer multiple points of access and require extensive security administration and support—ultimately translating into higher costs.

Develop policies, procedures and penalties (P3) in advance

By planning ahead and developing effective policies, procedures and penalties—known as the P3—you can help keep your applications and information secure. To avoid unnecessary obstacles, these should be enforced consistently.

Provide training on the use of the system, emphasizing the P3

Reinforce training by reviewing and publishing relevant news items, like attacks or system abuses. Keeping personnel properly informed and providing regular reminders can increase their retention rates and improve their understanding of critical security issues.

Use available security products rather than those developed in-house

Available products based on open standards have been tested and proven, and have customer references from which knowledge can be gained. Even if products are new, the methodologies used in testing can be evaluated and the results reviewed. Most importantly, industry-standard products are typically well documented for users and for IT technical staff.

Compartmentalize information, assets and users

Information assets require protection proportional to their value. Confidential informant files, intelligence reports and witness information must be carefully safeguarded, while public or easily replaced information does not require elaborate security. Accurately assessing data can help determine the most appropriate type of security system.

Inventory management. IT assets (e.g., personal computers, servers, hubs) and supplies (e.g., software, diskettes) must be appropriately inventoried and secured. Organizations often take delivery of large amounts of hardware and software without verifying the orders, ensuring that items are configured correctly and work properly, or entering items into an asset control database. When items are lost or fail to perform properly, there are no records to substantiate the loss to prove that the system is not performing as required.

Configuration control. Before any equipment is distributed to users, the configuration of every piece of hardware should be predetermined and all software properly registered. This information must be added to the inventory management system so that the inventory contains detailed descriptions of every system's components, hardware, software and location.

Problem reporting. This information is invaluable in tracking and protecting assets, identifying security breaches and conducting effective investigations when problems are detected. Industry-standard software can check configurations and automatically report problems to security administrators. This software can also maintain a log of system changes, upgrades or maintenance. Finally, locking mechanisms for workstations can reduce theft or tampering.

Supply and asset management. Supplies and assets should be treated according to their cost or importance, yet often this area is neglected. For example, organizations lock up inexpensive supplies while mission-critical assets are left unprotected.

User control. People should only have access to applications and information required to perform their job function. Even if approved for access to a restricted file, a user can be limited to viewing it from a certain workstation at a specific time. Organizations should also control who can create accounts or add users to the system, and audit the system frequently for dummy IDs or accounts.

System documentation. One of the most frequently overlooked security threats relates to system documentation, which can often be found in open, unsecured offices. While it may seem convenient and less expensive to prepare and publish standard documentation, it can be dangerous to system security. Widely distributed end-user manuals often contain large amounts of technical information that is highly valuable to a hacker. Someone armed with detailed systems information can attack with surgical accuracy instead of resorting to more easily detectable attacks. Publishing documentation on a network instead of in print can greatly reduce the security threat, while reducing costs and simplifying updates.

Realistic security administration objectives

No organization can set up or administer a completely impenetrable IT security program. Therefore, an organization must balance between desired and realistic goals. In-house staff can be utilized based on an assessment of what they can accomplish, while additional resources may be outsourced. There are many resources available to meet security needs that can be obtained from private companies at competitive costs. There is also value in resourcing—the symbiotic relationship between criminal justice agencies and members of the community. Sharing resources, pooling assets for joint acquisitions, donated services from universities or from the community are all potential ways to close gaps in a security plan.

Test, audit, inspect and investigate sites continuously and randomly

Regular updates to background investigations, use of voice stress analyzers, interviews and tip programs can help keep system security under control. In addition, organizations should implement methods for reviewing and testing code to protect against back doors into systems. Other approaches include:

- Using automated auditing and monitoring programs
- Publicizing threats and responses to them
- Taking swift, consistent and appropriate action when violations are detected or reported
- Using programs that check for file changes
- Advising employees that disciplinary actions will be taken in IT security cases.

Using emerging technologies to enhance security systems

IT security is rapidly advancing, but to be effective it must be properly deployed. Today, security features are available in almost every commercial, off-the-shelf application. Firewalls are increasingly powerful, adaptable and reasonably priced. Encryption programs are becoming more powerful and easier to implement and maintain. The ability to manage and monitor distributed systems from a single point in the network is steadily improving. Automated monitoring and audit programs to control system use and alert security administrators to attempted abuses are readily available. As these technologies continue to evolve, IT security will continue to improve in terms of effectiveness and ease of use.

Conclusion

The dramatic increase in the use of IT has exposed organizations to attacks on their information systems, assets and databases. Contrary to popular belief, the real threat rarely comes from outside sources, such as hackers. Unfortunately, protecting against this misperceived threat is expensive and ignores the real danger of intentional or accidental security breaches from internal, trusted sources.

However, with proper attention given to planning and implementing IT security, law enforcement and criminal justice organizations can prevent the vast majority of system penetrations. Planning based on a realistic assessment of security needs and threats, followed by the implementation of a well-developed security plan, can provide effective and comprehensive protection against the majority of network security threats.

Relying on the experience of a global team

IBM Global Services is the world's largest business and information technology services provider. We help companies develop e-business strategies, and design and implement real-world e-business solutions to achieve business results in this rapidly changing, competitive environment. The security and privacy experts at IBM combine skills in forward-thinking, creative problem solving; innovative technologies; and implementation to help you gain a competitive advantage.

For more information

For more information on IBM Global Services, contact your IBM sales representative or visit:

ibm.com/services

For other leading IBM research, business strategy reports and white papers, visit:

ibm.com/services/insights

For more information about IBM Government Industry consulting, contact:

insights@us.ibm.com

References

[1] Adams, Douglas. *Hitchhiker's Guide to the Galaxy.* Ballantine Books, reissue edition. November 1995.

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Printed in the United States of America
02-01
All Rights Reserved

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.