

A White Paper

What Every Decision Maker Needs to Know About Buying Public Safety Software Systems

January 10, 2005

**Prepared by: Alliance Technology Service, Inc.
W158 N 7738 Deer Trail
Menomonee Falls, WI 53051
262.255.0189**

Publicsafety@thatsbrilliant.com

This document is copyrighted by Alliance Technology Service, Inc. It may be freely distributed by Public Safety and Government agencies but not commercial entities without the expressed written permission of Alliance Technology Service, Inc. It is available for download from www.thatsbrilliant.com

Abstract: Research paper regarding Public Safety Computer Information Systems including Computer Aided Dispatch “CAD”, Records Management Systems “RMS” and the dynamics of identifying the right system for any size/type government entity. This paper attempts to uncover hidden costs and pitfalls of new and existing systems. The paper also presents new trends in pricing and business models that better accommodate communities facing tighter budgets and greater demand for services.

This document is copyrighted by Alliance Technology Service, Inc. It may be freely distributed by Public Safety and Government agencies but not commercial entities without the expressed written permission of Alliance Technology Service, Inc.
It is available for download from www.thatsbrilliant.com

Table of Contents

Abstract.....2.

About the Author..... 3.

Executive Summary.....4.

Public Safety and Computer Systems - Bridging the Chasm.....5.

Hidden Costs, Budget Eaters, and Tickets to Failure.....6.

The Trend toward Consolidation.....7.

What the Web did for Public Safety.....7.

Fault Tolerance and Disaster Recovery – Who Needs it?.....8.

The Tower of Babel –
Why is Information Sharing in Public Safety So Difficult?.....9.

New Business Models Enable Public Safety to Close the Gap.....10.

More Help on the Way.....10.

Summary.....10.

Glossary of Terms.....11.

About the Author

W. T. Klumb is the President and CEO of Alliance Technology Service, Inc. Alliance provides market analysis, technology valuation, expert witness testimony, and technology commercialization services to industries ranging from biotechnology, law enforcement, defense, satellite communications, telematics, environmental remediation, Brownfield development, automotive electronics and other heavily regulated industries. Alliance Technology Service, Inc. currently has 5 PhDs, in multiple disciplines advising clients.

Executive Overview

Public Safety and computer technology have both seen great change over the last 10 years. Unfortunately they have grown in different directions. Public Safety professionals have become more adept at protecting the public. Their role has expanded to include new threats such as terror attacks, infrastructure sabotage, copycat crimes, mobile and inter jurisdictional criminals, and unprecedented natural disasters. While information technology has grown to accommodate this larger role, the computer systems in your average public safety agency are nowhere near the sophistication commonplace in other industries.

This paper will explore why that gap is so large and what can be done to close it. This paper will analyze the past, present, and future issues facing public safety and computer technology, and attempt to explain why most computer systems have inadequately served public safety organizations. This paper reviews new developments and trends in Public Safety computer systems that increase the security of its citizens as well as preview new pricing models to better protect the buyer from failure.

Cost efficient public safety systems have grown out of reach for even the largest communities. Even with the expansion of grants and other funding methods, the conventional wisdom is that Homeland Security money will go towards putting more “feet on the street” and not computer hardware/software.

Public Safety and Computer Systems – Bridging the Chasm

Up until recently Public Safety has never fully benefited from the advances in computer technology. Most Public Safety organizations have always been several generations behind in technology. The average citizen would be shocked at the low level of technology most Public Safety agencies use today. This paper will look into the technological, financial, and political reasons for the large gap between current technology and public safety, and how to bridge that gap.

Information System Costs Are Supposed to Decrease Over Time – Right?

It is well known to us all that if we bought an IBM PC in 1985 and spent the exact same amount today, we would have about a 100,000% increase in speed, functionality and features. Today's software gives us much more for a lot less. Why? Competition has driven software prices down. More competition means more efficiencies and competitive prices. So, why doesn't this apply to public safety?

Since the Public Safety market is small compared to accounting, manufacturing, and most other professions, there is not enough market demand for large software companies to invest in a public safety solution. Smaller markets do not generate enough profit for software companies so they have to charge more to ensure profit. This leads to a less competitive market to deliver high end software that fits the needs and budget of most public safety agencies, and the communities they serve.

Most systems are developed, or custom built, for larger cities like New York or Chicago (cost +\$22,000,000) making it is hard to scale them back to fit jurisdictions with populations under 300,000. The cost to "customize" such systems could actually be more than the cost of the product itself. The outcome is rarely worth the effort or cost, with more incompatibilities surfacing as communities get deeper into the project.

The high costs of public safety systems forces communities to forgo important modules. For example, a community may invest \$500,000 in a records "RMS" and computer aided dispatch "CAD". This leaves them with incomplete systems and/or no interoperability with existing systems. These are known as "islands of operability" where Fire, Jail, Police and Dispatch operate autonomously on their own platforms, generally with no documentation of programming changes, and little or no opportunity for improvement. While this appears to be a viable low cost solution, the long term costs take their toll. Old and obsolete Public Safety systems generate higher MIS overhead with the perpetuation of aging and/or obsolete systems. Also, there is no appreciable improvement in performance, services, functionality, or productivity. In other words, the communities are paying good money to dig deeper into a hole.

In smaller to mid sized communities it is hard for government bodies to comprehend why the cost for public safety computer systems is so high. This makes it much harder for elected representatives to allocate money for public safety systems. Many aldermen, county supervisors, and the like, understand that the police need squads, radios, and guns,

while firemen need trucks, radios, hoses, and helmets. Governments resist spending hundreds of thousands of dollars to buy software, hire a system administrator, buy more hardware, and still not get the functionality or interoperability that the agencies need. They also see it as a lost opportunity to put more cops on the street, get the new fire truck, or replace some older squads.

Communities who do take the plunge are often upset with what they get, or don't get. There are actual counties that have spent over \$500,000 on a system that never really worked and then spent \$1,000,000 more to try and get it to work before abandoning the project altogether. That is \$1.5 million dollars wasted not including operational costs from years of going without a working system.

Another problem is that Fire, Police, and other Public Safety agencies buy their packages independently and have no interoperability with each other. This causes major frustration and expense when those agencies try to integrate those systems or move toward consolidated dispatch, within municipalities or counties. In many cases the cost to "connect" those systems is as expensive as purchasing a new system. Both options are cost prohibitive to meaningful change.

Hidden Costs, Budget Eaters, and a Ticket to Failure

What are some of the key issues regarding costs when buying Public Safety software?

1. Large Up Front Capital Expenditures – The upfront cost is usually so high that it makes it difficult to purchase necessary modules, deferring their purchase for another time. With an upfront cost of +\$200,000 communities are already committed to a system that is not yet up and running. If the system never lives up to expectations, communities are more likely to spend more money than to take a loss that large. Government entities rarely prevail over software companies in court. For some, the issue is saving face over a bad decision and not alienating or angering the taxpayers. When public safety agencies pay for a package before it is operational, the risk of success is squarely on their back.
2. Maintenance – Maintenance is a yearly fee that is often 20% of the purchase price. Maintenance is basically a service contract that ensures service after the sale. If a Public Safety package is \$300,000, the maintenance usually runs around \$60,000 a year. What this means is your community is buying the same package again every 5 years.
3. Hardware – Since most Public Safety systems are fat client, and not web based, they usually require an updated hardware platform and infrastructure to support it. This usually means significant capital outlays for faster and better computers as well as additional expense for upgrading operating systems and the programs running on that system. The hardware costs continue through the life of its existence through repairs, server upgrades, expanded disk drive, or storage capacity, etc.
4. Modification Fees – With proprietary "fat client" systems, changes, customization and modifications are inevitable. Very often these necessary modifications occur well into the conversion or installation process and are very costly. Most agencies

- neglect to budget for these changes and therefore get hit hard with fees that they cannot afford to pay or must defer to an indeterminate length of time.
5. IS Management Overhead – There are major costs associated with IS personnel working on Public Safety systems. Not only are valuable IS resources compromised by continually “fixing” or “patching” obsolete systems, your IS resources are not working toward solving other important community needs. While some IS managers could see this as an opportunity to “build their empire,” most would prefer to work on projects that move their skill set forward or advance the efficiency of their areas of responsibility.
 6. Productivity Loss – Your community can lose untold dollars on “dysfunctional” Public Safety systems by applying IS resources, and funding, to keep a weak system going. Needless to say these are resources that could be better utilized in your community.

The Trend toward Consolidation

Many government entities are considering or being forced to consolidate services with other agencies or communities. What sometimes prevents consolidation from actually taking place is the reluctance or inability to purchase the hardware and the associated costs that go with it. Other communities do not want to abandon their infrastructure to migrate to an unknown system. Many agencies are now considering using “Hosted Services.” Using hosted services gives any agency the ability to save costs on hardware, lower overhead, and better utilize IS personnel involved with maintaining those systems.

When an agency moves to hosted services, they eliminate the need for evaluating, buying, installing, housing, servicing, trouble shooting, software/hardware compatibility, upgrading operating systems, and diagnosing hardware incompatibilities.

A hosted services company can offer high quality hardware at a nominal price by spreading the cost of the system over many agencies. Each agency pays a fraction of what it would cost to purchase and run their own data center while the company hosting the services makes money through the economies of scale.

Another huge advantage to hosted services is the ability to have fail-over redundancy and instantaneous disaster recovery operations. The key to continuous operation is to have redundant internet connections (as the internet was originally designed to maintain communications in catastrophic event). The cost to establish a redundant data center for a single Public Safety agency is completely cost prohibitive.

What the Web did for Public Safety

Even though the web did not live up to the expectations of some investors, its positive impact on almost every business is indisputable. Public Safety agencies may benefit most of all because now, even the smallest agencies can actually afford many of the functions, features and interoperability that has eluded them for many years. The “ASP” model or Application Services Provider can provide cost effective and up to date applications from a central location to any authorized user with an internet connection. You see this model

working with online banking. A banking customer connects with the banks server and couldn't care less what version of software the bank is using because it does not affect the user. The banks do not care what kind of operating system their customer is using because it does not matter to them. It all works together through the wonder of the shared, yet secure, infrastructure of the internet.

The Tower of Babel – Why is Information Sharing in Public Safety So Difficult?

The need for Public Safety agencies to share information has been one of the greatest challenges ever imagined. Never has the need been greater but the obstacles are almost insurmountable. With all the responsibilities that Public Safety professionals have, information sharing remains a low (and unfunded) priority.

While there are many political and turf protection reasons for the lack of progress, the simple fact is that up until the web was fully developed there has never been a simple and affordable infrastructure they could use. Even when the web became commonplace, existing public safety systems could not communicate without extensive and expensive interfaces.

The Internet and Web were specifically built to address the needs of military, government, and essential agencies in catastrophic times. It makes perfect sense that it should be applied to all types of critical information sharing, especially public safety, in everyday use as well as in disasters.

Fault Tolerance and Disaster Recovery – Who Needs it?

If 9/11 did not convince the public and public safety agencies of the necessity for resilient, redundant and alternative off site recovery systems, the tsunami disaster did. Nobody can predict if, when, or what type of disaster will hit, but it will be the time when you will need your Public Safety systems the most.

Disasters will not always be on the magnitude of a tsunami. More common disruptions are backhoes severing power and/or communications. The biggest obstacle to having a redundant facility is cost. It is almost out of reach for any community to have their main center "armored up" to shield them from disasters, let alone have an identical data center a safe and reasonable distance away ready to go online in the event of a big problem.

Web based programs do not have this issue as long as there is a connection to the internet. A flood at the Sheriff's Department, resulting in their inability to dispatch could set up an alternative dispatch center at the High School or Library where there is working internet access.

New Business Models Enable Public Safety to Close the Gap

Several new business models have evolved that specifically address public safety. The computer hosting model and the fee for service model may forever change how public safety handles their MIS needs.

The first model is the “Computer Hosting Model” that takes the burden of selecting, maintaining, upgrading and replacing in house computer systems and puts it on a private company’s shoulders. It frees up manpower and in some cases precious physical space and puts the uptime burden squarely on the shoulders of the vendor. Security issues are always a concern, but the reality of today’s hosted services puts law enforcement and public safety data in a more secure environment than Banking, which traditionally has been the most security conscious of all industries. A substantial number of banks in the US do not have their data on their own computers or servers anymore: yet have total access to customer records.

Another huge leap and benefit for Public Safety agencies is the “Fee for Service Model” which spares government entities the risk of huge capital outlays on systems that do not live up to what was promised. In the fee for service model the government entity pays a yearly fee to the service provider. That fee is usually determined by the population, number of Public Safety agencies on the system and the number of modules used, such as Records, Fire, CAD, Booking, Jail, Public Works, etc. With this model there is not a large up front expenditure required to consummate the contract.

The fee for service model makes it easier for common councils and county boards to spend \$50,000 to \$150,000 per year rather than to get an approval for a \$300,000 to \$700,000 up front expenditure, with a yearly maintenance contract of 20% each year. It is very hard, if not impossible to get out of your contract if it does not live up to expectations.

The key element that makes this model attractive to government agencies is that it greatly reduces the risk of making a bad decision. Second, it allows for the agency to rectify the decision much more easily. It also ensures that your vendor will have your customer satisfaction high on their list of priorities. Many companies will not start to see any profit until well into the second year of the contract and want your business for years to come.

The other side of that benefit is that if your agency is, or becomes, unreasonable the service provider will greatly raise your fees to cover their excessive services commitment to you. Some companies may prefer to see you leave (and raise their prices accordingly) so they can concentrate on existing reasonable customers or find a replacement for your agency.

An unintentional byproduct of this model may be that it can expedite the process to get a working solution in any agency. When any business or government agency can see an 80% cost savings over buying a package, the hardware to run it, the staff to keep it

running, the maintenance fees to keep it up to date, never replacing the hardware, etc. it becomes almost axiomatic that the fee for service model should at least be used as an interim solution at worst: and a long term effective, pragmatic, and cost saving solution at best.

More Help on the Way

With the rapid advancement of Voice over Internet Protocol commonly referred to as VoIP, voice communications and interoperability will improve another large problem for Public Safety had endured since the advent of the radio. Web based systems will have a great advantage over traditional legacy systems in converging voice and data communications. Yet again, the Web, via Internet Protocol, will provide public safety with the tools it has always needed but could not afford.

Summary and Conclusions

While computerized information systems have been a boom for just about every industry and government agency, public safety has realized a fraction of that productivity and information sharing. The greatest technology available is only accessible if it is within your budget. Many Public Safety systems that are affordable would not meet the bare minimum standards of the average small business.

The role of public safety has grown over the past 4 years. The public better appreciates what they do but, these agencies are faced with a larger universe of dangers, preparedness, and responsibilities. Along with the growth of their role is the other unfortunate reality that there will never be the financial resources available to equip them with all the tools they need.

Existing Public Safety computer systems are moderately effective for the largest communities and overpriced, or out of reach, for smaller communities. Combine that with hardware costs and overhead, the first responders are left with a smaller piece of the pie for squads, fire trucks, radios, bio hazard suits, and other essential items.

New technologies that tap into the advantages of the World Wide Web, Application Services Providers, and the amazing power of the desktop/notebook computer has bridged the gap that has long existed between public safety and the private sector.

New business models such as Application Services Providers, Fee for Services, and Hosted Computer Services, work well within the budgetary constraints of most public service agencies.

As with any technology, new or old, choose carefully and wisely. The information in this paper should assist you in making the right decision for your Public Safety agencies and your community.

Glossary of Terms

ASP – Application Services Provider is a “software vendor” that offers applications via the internet instead of having a “fat client” resident on your desktop or company server. All of the software is resident on their server which eliminates the burden of updates and changes on the client.

CAD – Computer Aided Dispatch - A method of using a computer system to assist a dispatcher for police, fire, emergency medical teams, and even public works, units to dispatch public safety resources in the most rapid and effective manner possible. CAD is a tool that assists a dispatcher taking calls from citizens and generating the correct action with the available and closest resources. A fully operational and integrated CAD system will save lives and reduce property loss.

Consolidated Dispatch – A recent movement toward sharing and consolidating resources in public safety by consolidating the dispatch center in a central location as opposed to having each community have their own dispatch center. This coincides with various communities considering combining regional fire, EMS and other services.

Fat Client – Proprietary software that resides on a network server or is resident on every desktop computer. Microsoft Office is an example of a fat client.

Fee for Service Model – A new business model that reduces the risk to a community by paying a yearly fee, instead of requiring a large up front expenditure to acquire public safety software. This model puts the performance responsibility on the vendor to provide satisfactory service in order to continue to receive the annual fee for service.

Hosted Computer Services – Where the computer is usually located off site and maintained by a separate entity, usually from the private sector. The company responsible for the hosting services is responsible to fixing, maintaining, upgrading and back up service. The advantages are reduced or eliminated hardware costs, lower overhead in the way of system administrator(s), lower software licensing fees, lower utility bills, more space, and more money towards other items.

RMS – Records Management Systems - A fully functional RMS system will provide all public safety agencies with accurate information about individuals, property, hazards, dangerous intersections or strips of roads and crime reporting to state and federal agencies.

Web Based Public Safety Systems – Computer or MIS systems that are operated over the web instead of on computers residing on premises using proprietary fat client software. The benefits of web based systems are the elimination of massive and costly hardware infrastructure, and personnel expense. Updates and modifications occur on web servers without requiring client time or more resources.