

KEEPING PEOPLE SAFE:

*HOW INTEGRATED SECURITY NETWORKS
ARE MAKING COMMUNITIES SAFER*



THE GOALS OF THIS WHITEPAPER ARE TO EXPLORE:

- ✓ the rapid change and dynamic nature of the public safety threat matrix;
- ✓ the ways in which past approaches to safety and security are becoming outdated; and
- ✓ emerging models for integrated security that are meeting today's challenges.

Security-over-IP (Internet Protocol) is an emerging approach to safety and security that links traditionally isolated systems for physical and cyber-security together via a secure broadband network. This linkage creates a network effect between the previously separated systems, dramatically increasing their value for threat detection, mitigation and recovery. The benefits of Security-over-IP are more comprehensive pictures of emergency situations, faster re-tasking of critical resources and better coordination of inter-jurisdictional response efforts.

Threats to personal safety and security, whether they be natural disasters such as hurricanes or tornadoes, or man-made attacks such as shooting sprees or terrorist activities, can have a disastrous impact on our lives and the lives of our loved ones. Communication during and after these threats is critical. In the past, disparate response systems could cause confusion and even make the situation worse, but the case is quite different with integrated, state-of-the-art security networks.

SHOTS FIRED: THE CHANGING PUBLIC SAFETY THREAT MATRIX

Government has been in the business of protecting people from physical harm for a long time. Adam Smith, writing in 1776, said that the first duty of government was to protect people from physical violence and the threat of military invasion. This concept of government as the guarantor of personal security is enshrined in the founding principles and documents of practically every society, and its earliest references date back thousands of years. The oldest known written laws, including the 4,000-year old Mesopotamian Codices of Ur-Nammu and Hammurabi, placed the security of the people from physical harm at the apex of government's responsibilities.¹ After more than 4,000 years of trying, one may be tempted to think that the problem of public safety has been solved. Think again.

In April 2007, 33 lives were lost at Virginia Tech in what *The New York Times* called "the most deadly shooting rampage in American history."² As a nation, we stood in horrified silence as a lone gunman took lives and paralyzed an entire college campus. Responders from several independent groups came together, including local officials, campus police, parents and even the federal government.

The Virginia Tech Review Panel's August 2007 final report noted that "Virginia Tech and Blacksburg police departments responded quickly to the report of shootings ... as did the Virginia Tech and Blacksburg rescue squads. Their responses were well coordinated."³

While the coordination between law enforcement units was commendable, the wider response to the emergency was not sufficiently integrated. The same report noted that the university "failed to issue an all-campus notification about [the first shootings] until almost two hours had elapsed," which was considered unacceptable. Post-emergency support systems

were not well linked to the rapid response capabilities of the law enforcement agencies.

“State systems for rapidly deploying trained professional staff to help families get information, crisis intervention, and referrals to a wide range of resources did not work,” the review noted. Overall, the review panel made a key recommendation in favor of better integration of response and recovery activities: *“In order to advance public safety and meet public needs, Virginia’s colleges and universities need to work together as a coordinated system of state-supported institutions.”*⁴

While some communities may be relatively safe from the type of violent crime displayed in the Virginia Tech incident, practically everyone is vulnerable to extreme weather and natural disasters. Hurricanes show no sign of abating, and we see continued threats from extreme cold, tornadoes, earthquakes, floods and wildfires. The responses to the more recent Hurricane Gustav and Hurricane Ike demonstrated that many lessons of the Katrina experience had been learned, but they also proved that the threat of lost lives and massive property damage have not disappeared from our threat landscape. Despite a successful evacuation, Hurricane Ike still clobbered the Texas coast with an estimated \$29.4 billion in property damage.⁵

The latter months of 2008 showed that other types of threats to safety and security had not diminished. A government mailroom in Michigan received white powder in a suspicious package intended for Michigan Gov. Jennifer Granholm.⁶ By December, more than 30 envelopes containing white powder were sent to governors’ offices around the nation.⁷ While the packages ultimately turned out to be harmless, the incident was eerily similar to the anthrax attacks on the U.S. Capitol several years ago.

In addition to crime and natural disasters, government and educational officials may also be called upon to respond to riots or other temporary breakdowns in civil order. While these events usually begin with an isolated incident, they can quickly spread to involve large groups of people in otherwise safe communities.

In 2005, a single event touched off 200 nights of rioting in Paris that ended with “8,973 vehicles torched; 2,888 arrests; and one person dead.”⁸ The 2005 riots became an important topic in the subsequent French presidential

election and were a major backdrop of incoming President Nicolas Sarkozy’s domestic policy agenda.⁹

In another example, this time from December 2008, Greek police failed to contain more than a week of violent riots that paralyzed large portions of that country and ultimately required a coordinated national response.¹⁰ Even Iceland — which had been rated the “most peaceful nation on Earth” by Britain’s Economist Intelligence Unit only six months earlier¹¹ — experienced violent protests after the collapse of the nation’s major banks.¹² It is likely that most government planners in Iceland had not included “rapid decline in the value of U.S. equities” as a threat vector in their public safety planning. If a similar scenario seems farfetched for the United States, consider that the U.S. ranked 97th out of 140 countries in the same survey that called Iceland the most peaceful nation on Earth.

As these threats seem to multiply all around us, technology seems to be taking a bigger role in how they play out. Witness the deadly Mumbai terrorist attacks, which killed at least 174 people and riveted the world. Security analysts unanimously agree that these deadly attacks would not have been possible without the advanced consumer electronics on the market today. Noah Shachtman, writing for the *WIRED* Magazine blog network, said that “the Mumbai terrorists used an array of commercial technologies — from Blackberries to GPS navigators to anonymous e-mail accounts — to pull off their heinous attacks.” What is more troubling is that Shachtman noted that “in 2007, former U.S. Central Command Chief Gen. John Abizaid complained that, with its Radio Shack stockpile of communications gear, ‘this enemy is better networked than we are.’”¹³

“Unfortunately, those determined to strike terror into the influential will likely continue to target opulent ‘softer’ targets as they did at the Serena Hotel in Kabul, Afghanistan, in January 2008 and the Taj Mahal Palace in Mumbai, India, in November 2008,” said Security Analyst Joseph Maida IV. Maida has a state and an international perspective on the issue of security, since he served as an assistant attorney general for the state of Texas and as a criminal justice advisor for a private sector company working through the U.S. State Department in Herat, Afghanistan.

The proper response for the good guys is *coordination*, according to Maida. In his words, “Integration of intelligence from reliable sources as well as coordination between police and private sector security infrastructures will be increasingly important.”¹⁴

FROM COMPUTER SECURITY TO CYBER WARFARE

A great deal of good work has been done and progress has been made with IT security. For instance, the state of Texas reported that it successfully defended against more than four million malicious intrusion attempts into the state's Web portal and blocked between "300,000 to 500,000 SQL Slammer worm events per hour on the state's capital area network."¹⁵

Despite these successes, much work remains.

"We are seeing an explosion in cyber threats," said Dan Lohrmann, former founding director of Michigan's Office of Enterprise Security and state chief information security officer (CISO). "The total number of reported data breaches doubled last year (nationwide) according to the Privacy Rights Clearinghouse."

"THE THREATS RANGE FROM NAÏVE, IGNORANT AND CAVALIER EMPLOYEES IGNORING RULES AND MISUSING SYSTEMS TO REAL, NO-KIDDING BAD GUYS TRYING TO COMPROMISE OUR APPLICATIONS AND DATABASES."

Mark Weatherford, executive officer of the California Office of Information Security and Privacy Protection

To Lohrmann, this means that more identity theft is happening in society, and that we are seeing more sophisticated attacks from professional hackers and organized crime.¹⁶ These external threats, however present on our minds, are only part of the picture.

In July 2008, Terry Childs, a rogue systems administrator working for the city of San Francisco, locked the entire city government out of its own network.¹⁷ Ron Vinson, deputy director of San Francisco's Department of Technology Information Services, told *WIRED* Magazine that Childs "had the trump card and he could have brought everything down if he wanted to."¹⁸

Even unintentional acts can threaten government systems, as noted by the Texas Department of Information Resources (DIR) in a recent report. "For example, insiders have introduced

viruses into state network resources by placing contaminated disks into the systems and by downloading contaminated Internet attachments. These unintentional insider-facilitated attacks provide malicious outsiders an open door to the network through the Internet that they can use to extract sensitive information or launch additional attacks."¹⁹

In total, the Identity Theft Resource Center's "2008 Breach List" reports that more than 35 million records containing sensitive, personal information were compromised in the United States in a single year.²⁰ Mark Weatherford, executive officer of the California Office of Information Security and Privacy Protection, describes the threat environment faced by his organization as "relentless."

"The threats range from naïve, ignorant and cavalier employees ignoring rules and misusing systems to real, no-kidding bad guys trying to compromise our applications and databases," said Weatherford.²¹

Weatherford also notes astutely that cyber-security is covering much broader ground than it did even five years ago. Weatherford "believe[s] government needs to become more directive in mandating upgrades to the technologies of some of the more historically static environments such as power generation and distribution, transportation, oil and gas pipelines, water distribution and even telecommunications. The digital interdependencies and remote management capabilities of our nation's critical infrastructures have grown dramatically in the last decade. There is a huge cyber-security risk to those environments and our national security and the subsequent economic consequences to our nation."

Cory Ortigoza is a homeland security analyst who has advised Congressman Kevin Brady (8th District of Texas), organized Houston's first Department of Homeland Security Community Emergency Response Team and participated in the development of a conceptual framework for domestic pandemic situational awareness. Ortigoza said that cyber war between nations — whether it happens officially or through proxy groups — is a "hot emerging area" in the field of public safety and should be incorporated in national planning scenarios.

"We used to call cyber attacks 'weapons of mass disruption,' because their primary intent was not to kill. But that is changing, because the secondary and tertiary effects can be just as deadly."²²

HOW THE PUBLIC SECTOR THREAT MATRIX IS CHANGING

“What we are now seeing is a convergence of threats,” said Texas Homeland Security Director Steve McCraw. While law enforcement bodies, critical infrastructure protection teams and a host of other resources aimed at preserving the safety and security of citizens have been in place for years, today’s threat is more dynamic and more integrated than ever before.

“Threats don’t target specific jurisdictions,” said McCraw, “and they don’t care where we happen to draw our organizational boundaries.”²³

Maj. Dean Hairston, commander for the city of Danville Police Department in Virginia, noted the same issue in a recent whitepaper he co-authored. He described a situation in which a criminal was engaged in a high-speed chase near the North Carolina border after committing a crime in Virginia. Before Hairston’s team took action by implementing a new, interoperable communications system, there was no direct connection between the law enforcement jurisdictions. In the past (before the new system was implemented), the situation worked like this:

“The Danville dispatcher dials long-distance to the Caswell County, N.C., dispatcher, who informs county officers that a fleeing suspect is about to enter their jurisdiction. Unfortunately, when the suspect crosses the state line, the officers in Virginia have to drop their pursuit, and their counterparts in North Carolina are not notified in time to pick up the chase. The suspect escapes, just as he had anticipated, because he could exploit the incompatibility of inter-agency communications.”²⁴

While there may be as many methodologies for categorizing security threats as there are practitioners, we can break down the public safety threat matrix into five key verticals: 1) crime and social unrest; 2) extreme weather events; 3) terrorism and foreign wars; 4) public health emergencies; and 5) cyber attacks. Each of the five verticals is seeing its own dramatic degree of malleability as threats show an ever-increasing ability to evolve and “mutate” to fit changing response tactics. As the change with each vertical has accelerated, the level of integration between threat verticals is also increasing. Terrorism in particular, especially as it

might become super-charged during a war between nation states, shows a dangerous ability to break out of its vertical to affect other areas.

Interestingly, McCraw sees technology as part of the problem — and part of the solution. “Since the 1990s, the technology revolution has been one of the chief drivers of globalization. Just as technology was a force for the globalization of our economy, it has also globalized crime. Change affects both the best and the worst parts of our society. As we see this convergence of threats — especially between crime and terrorism — we see crime that had traditionally been local is extending its reach.”²⁵

McCraw is right: We now live in the fastest and most interconnected society in history, and we have reaped countless benefits as these changes have swept through

HOW DO YOU PRIORITIZE THREATS WHEN EVERYTHING IS CRITICAL?

Texas Homeland Security Director Steve McCraw favors the RAND model for prioritization, which is based on an estimate of the expected impact of a threat situation. The model was developed by the RAND Corporation, a non-profit institution that conducts research on a variety of areas, including defense and national security.²⁷ “In the RAND model, risk equals the threat times the vulnerability times the consequences.”²⁸

“For example, consider the risk of a Category 3 hurricane making a direct hit on Galveston Island. The threat of that occurring is low — it has only happened a few times in the past century — but the vulnerability is high and consequences are beyond catastrophic,” said McCraw. “So that is a scenario that ranks very high in our regional and statewide planning.”²⁹

**Risk = Threat of Occurrence
times Vulnerability
times Severity of Consequences**

the disciplines of education, commerce and daily life. While the rapid advancement of technology has led to wonderful breakthroughs, it has also put unheard of capabilities in the hands of criminals, hackers, terrorists and other malcontents. If Thomas Friedman is right that globalization is making the world “flat,”²⁶ one must assume that the effect works for the bad guys as well as the good guys. Public officials at all levels of government face an increasingly diverse and dynamic threat matrix that is challenging them to work in new ways.

CONNECTIONS AND DOTS: WHY A PIECEMEAL APPROACH NO LONGER WORKS

In the past, new types of threats and new response capabilities emerged slowly. The types of threats were fairly isolated, and the technology used to detect, respond and recover from them was highly specialized and proprietary. As the number and types of threats to public safety multiplied, so did the systems used to manage them.

Public officials are now expected to preserve existing investments in video camera systems, law enforcement radios and fire suppression systems while adding myriad new capabilities for cyber-security, event correlation and response to chemical, biological and radiological threats. Examples of these traditionally closed systems that address a specific threat include:

- video surveillance;
- gunshot detection;
- fire suppression and water intrusion;
- cyber-security and computer network protection;
- law enforcement communications systems; and
- chemical, biological and radiological agent detection.

It is important to recognize the investment and the success of these systems. McCraw noted, for example, that “before you can have *interoperability*, you first must have *operability*.” These first-generation solutions went as far as they could, but they are closed, proprietary systems that deal with isolated threats.

The problem is existing systems have a foundational design assumption that no longer holds true. In the past, we assumed that threats came one at a time — that you would not, for example, have a crime and a public health

INCREASING NEED FOR ADAPTABILITY OF SECURITY NETWORKS

“No plan survives first contact, and you have to adjust with conditions as you face them,” said Security Analyst Cory Ortigoza. He points to the need for adaptability in the response by state and local government officials when responding to an emergency or security threat. This flexibility to respond to change threats needs to be built in to the government’s capability to respond.³¹



emergency happening at the same time as a major storm. The reality is that integrated threats do exist, and that they are becoming more prevalent. Legacy systems for video surveillance have been in place for many years, and they are typically used for a single purpose. Rarely has the data from one system been able to coexist with others. Unfortunately, our tactics have not kept pace with the changes in the threat environment.

“An integrated approach to safety and security has been badly missing, even since 9-11,” said Security Analyst Cory Ortigoza. “Jurisdictional issues must be overcome, but getting over them will be a continuing problem. The integrated approach needs to accelerate. We need to break down these firewalls between jurisdictions and begin working together.”³⁰

If you’re still not sure about the level of integration between security threats, consider this exercise. When someone says “port scanning” today, we can’t immediately tell if they are talking about IP packets entering a computer system or shipping containers hitting the docks. In today’s world, we might actually be talking about both at the same time. With complex, integrated and rapidly changing threats on the landscape, the past approach is outdated and insufficient.

A NEW APPROACH: CONVERGED SECURITY NETWORKS

WE ARE ALL FAMILIAR WITH VOICE-OVER-IP BY NOW; GET READY FOR SECURITY-OVER-IP.

Imagine the future: a converged security network that links varied devices, collects information in real time, has powerful event correlation capabilities, and allows a coordinated response from government across multiple jurisdictions. Does it sound too good to be true? It's not, and it's happening today.

Innovative government officials are paving the way for successful adoption of converged security networks, while preserving the need for privacy and the respect of jurisdictional boundaries. While the full vision has yet to be realized, excellent progress is beginning to link legacy systems with powerful, Internet-age systems built on a converged IP platform. We are all familiar with voice-over-IP by now; get ready for **Security-over-IP**.

Consider this example as a thought experiment: a gun is fired a few feet away from an elementary school, and citizens rightly expect a public safety response. In the past, this might lead to the deadly confusion seen in the Virginia Tech experience, or worse, the Mumbai shooting. But the case is quite different with a state-of-the-art converged security network.

In a converged scenario, the gunshot is detected by a specialized sensor placed in the high-risk area near the elementary school. Security cameras — with video and audio capability — are automatically repositioned to get a better view of the area of the shooting. Data from the front line detectors is piped via an IP-based network to an event correlation system that concludes the event is of major importance. In an instant, the same IP-based network sends alerts to school officials, city government, local police and homeland security. Responders with multiple types of equipment from different manufacturers begin to communicate seamlessly. A coordinated response begins, with each government branch responding in its own

particular way, but making use of the same data. The school is locked down and the SWAT team is on its way — all before anyone has the chance to call 9-1-1.

“You can't prevent everything,” noted Security Analyst Cory Ortigoza, “but you can reduce the time needed to respond.” Add to that increasing the quality of that response, and converged security networks become a powerful force multiplier.

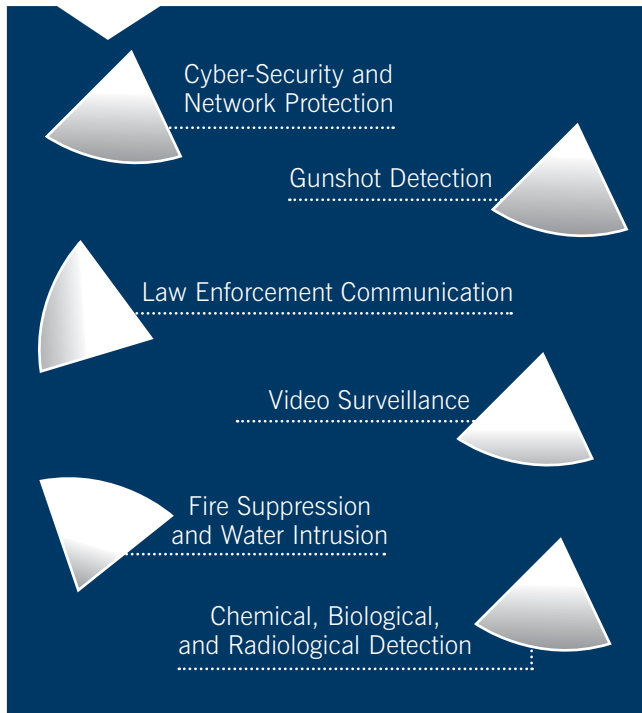
The result is a system that is more resilient, more adaptable and better able to respond to the diverse threat environment of today. By building on the power of an IP network, security reaps many of the benefits gained by Voice-over-IP — connections of multiple devices, robust interoperability and plug-and-play adaptability.

KEY COMPONENTS OF AN INTEGRATED SECURITY NETWORK:

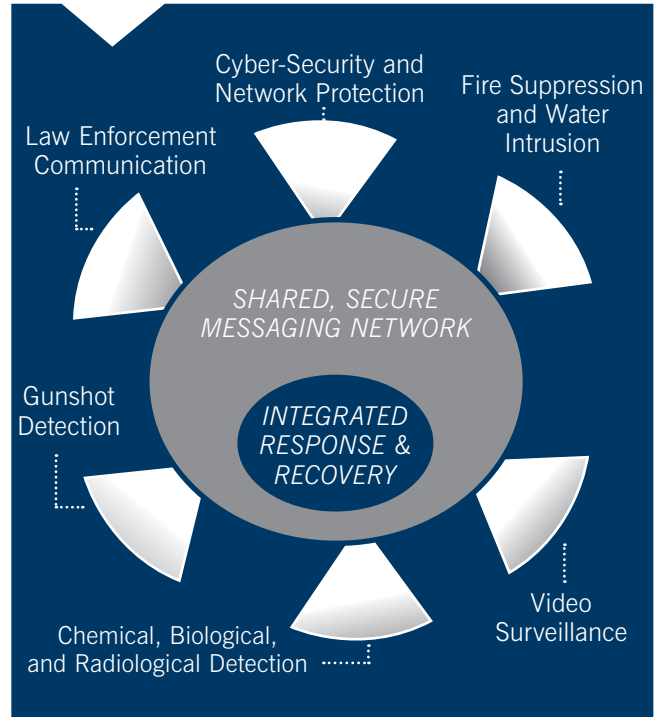
- ✓ Distributed sensors to detect diverse hazards
- ✓ A common data network to connect the disparate detection devices
- ✓ Integrated response systems — with event correlation capability — to make sense of the data
- ✓ Strong network security to prevent unauthorized access
- ✓ Resilient infrastructure that can survive adverse conditions



BEFORE: SILOED, JUMBLED



AFTER: AN INTEGRATED SECURITY NETWORK



PROTECTING CITIZEN PRIVACY AND RESPECTING ORGANIZATIONAL BOUNDARIES

Importantly, this type of technical integration allows policymakers to improve safety and security while protecting citizen privacy and respecting established jurisdictional boundaries. This integrated network model for security is not only better in terms of technology, it is also firmly grounded in the realities of inter-governmental cooperation. In fact, thought leaders answered with a resounding “no” when asked if they recommended changes to the literal jurisdictional boundaries between different government entities.

“Jurisdictional boundaries exist for a reason, and each agency matters,” said Texas Homeland Security Director Steve McCraw. “We put the resources to respond in the local jurisdictions, expanding the capacity of the first responder. Then you layer on top of that a regional and statewide capability for planning and incident response.

The combination of those actions ensures that we can draw resources together in the event that one jurisdiction becomes overwhelmed.”

In addition to respecting operational boundaries, citizen privacy is of great concern. “The privacy of citizens is paramount,” said McCraw. “We can’t just collect data for the sake of collecting it. The technology may be there, but it needs to be used in a responsible way that the American people are comfortable with.”

GOVERNMENT AND EDUCATION ARE SEEING THE BENEFITS

While the concept of an integrated security network is relatively new, government and education officials are beginning to realize the benefits of an integrated approach to security. Here are some examples:



JOHNS HOPKINS UNIVERSITY INTEGRATED GUNSHOT DETECTION SYSTEM

Johns Hopkins University, located in Baltimore, Md., recently deployed an integrated system that can detect gunshots and instantly route the information to several different law enforcement entities to support a coordinated response.

The system begins with specialized sensors that are placed on the school's Homewood Campus and surrounding areas that are tuned to detect a gunshot. When a gunshot signal is detected by a sensor, the message is wirelessly transmitted to a receiving base station. The base station then relays the message in real time across a secure channel on the campus' network. The gunshot's location and the nearest address is then displayed on a 40-inch LCD screen in a campus security response center. The Johns Hopkins University Police then notify the Baltimore Police Department, and an integrated response can begin.

While there have thankfully been no gunshot incidents since the system was installed, the campus can rest assured knowing that both the Johns Hopkins and Baltimore police departments will be in response mode as soon as a shot is fired.³²



SAN DIEGO SHERIFF'S DEPARTMENT

In October 2007, San Diego County faced a series of devastating wildfires. In response to this challenge, the Sheriff's Department deployed a Network Emergency Response Vehicle (NERV) that served as a mobile command center. The NERV was a rolling package including an IP Interoperability and Collaboration System (IPICS), links with landline unified IP phones, a Wi-Fi network, PCs, and a state-of-the-art telepresence solution.

Lt. Margaret Sanfilippo of the Sheriff's Department said that "by providing us with comprehensive communications capabilities, the NERV enabled us to allocate our resources properly, deploy them more quickly and conduct our mission in a safer manner. The NERV made it much easier for me to manage people and resources."

Capt. Guy Chambers of the Sheriff's Department went further. "I can unequivocally say that the NERV was instrumental in helping us manage the Harris Fire properly," he said. "Without it, we probably would have lost structures and lives."

"IP IS THE FUTURE. THERE ARE NO IFS, ANDS OR BUTS. THAT IS WHERE EVERYONE IS GOING."

Steve Jennings, CIO of Harris County, Texas



STATE OF TEXAS DISASTER RESPONSE TRACKING SYSTEM

The experiences of hurricanes Rita and Katrina taught Texas emergency responders a great deal, and one of those lessons was that it is difficult to track assets and people in the event of a large-scale disaster. State officials were particularly concerned with ensuring the safety of special needs evacuees during an emergency. As a result, they deployed GPS-tracking devices to buses that would be used for evacuations, as well as an ID bracelet system with radio-frequency identification (RFID) tags for ensuring the safety of special needs evacuees. This allows responders to “track assets and people in real time across the state” when the need arises, according to state Homeland Security Director McCraw. This connection of information across law enforcement, recovery workers, cities, counties and the state led to much more effective evacuations, especially for those vulnerable because of special needs.

BENEFITS OF INTEGRATED SECURITY NETWORKS

- ✓ comprehensive picture of an emergency situation;
- ✓ better capability for expansion and change over time;
- ✓ rapid re-tasking of resources in the event of changing threats; and
- ✓ better overall effectiveness and return-on-investment (ROI).

PIEDMONT REGIONAL VOIP PILOT PROGRAM (RVIP)

Several independent jurisdictions in Virginia faced the daunting and well-worn task of establishing radio interoperability between their networks. While the typical approach might be to upgrade everyone to the same land mobile radio (LMR) technology, this strategy was highly cost prohibitive. Instead of taking the common and highly costly approach, the participants deployed an IP-based Interoperability and Collaboration System (IPICS). This linked not only the various radio systems, but also provided interoperability capabilities for landlines, VoIP phones, and



cellular devices. According to a report co-authored by Maj. Dean Hairston of the Danville, Va., police department, “The Piedmont RVIP project validates an exceptional model to improve local and state public safety response effectiveness through the use of IP technology. For the first time ever, these organizations are able to communicate in ways that they never thought possible. We recommend that all sovereignties look into taking full advantage of their existing IP network infrastructure to improve both inter- and intra-jurisdictional communications.”

FEATURED CASE STUDY: PUBLIC SAFETY INTEROPERABILITY IN HARRIS COUNTY, TEXAS

Steve Jennings, longtime CIO of Harris County, Texas, has been a trailblazer for the cause of public safety interoperability. Perhaps he had to be, considering the size and scope of his own jurisdiction. Harris County is home to more than four million people, the largest city in Texas and 1,778 square miles of land. The county faces a multitude of public safety threats, since it is large and diverse in every sense of the word. NASA's Johnson Space Center is located there, along with several universities and much of the nation's critical energy infrastructure. The terrain is varied, encompassing metropolitan as well as rural areas. Forty-nine square miles of the county are covered in water, and it is centrally situated on the hurricane-prone gulf coast.³³ Add to that the growing need for coordination with other counties and cities in the surrounding areas, and it all adds up to quite a challenge.

Where to start? Jennings begins by stating the problem. "First, we have to define what public safety is. At the federal and state levels, 'public safety' usually means law enforcement. But public safety is not just law enforcement. We define public safety as 'the protection of the general population from all manner of significant danger, injury, damage or harm, such as may occur in a natural disaster or calamity.'"

Jennings noted that the responsibility for public safety is broad, and touches nearly every government and educational institution in the area. There are "police, fire/rescue, emergency medical and ambulance" for starters. "But public health is a part of it as well, as are the schools and the school police forces. We have a level one trauma center, which is one of the finest medical facilities in the world. Even public works is part of this, when they are called upon to move debris." Jennings goes so far as to include the

public itself in his inventory of response capabilities, as it is organized with the 53,000-member Harris County Citizen Corps that plays a role in emergency recovery. All of this adds up to many different players, and a clear need for coordination and interoperable communications.

TECHNOLOGY INTEROPERABILITY PLAYS A CRITICAL SUPPORT ROLE

According to Jennings, a successful response to a disaster or emergency situation involves three things: "awareness, direction and reassurance." Jennings is careful to put his primary focus on leadership, noting "we have a strong county judge and strong commissioners who communicate with the people, direct the people, and reassure them in the event of a crisis." But he also highlighted the vital support role that technology plays in any public safety incident.



Jennings' and his team's work has paid off, and Harris County has become the backbone of regional disaster response. They operate one of the largest interoperable radio systems in the nation via a cooperative arrangement that covers a substantial

portion of east Texas. The county has been especially effective in natural disasters, including the recent Hurricane Ike when they successfully evacuated 2.3 million people in 24 hours. How did they do it? Technology was a big part of the answer.

“The regional radio system has been a godsend, because it eliminates the biggest problem in an emergency, which is the lack of communication,” Jennings said.

The county also played a critical role in the recovery effort after the Space Shuttle Columbia disaster, earning recognition from then-NASA Director Sean O’Keefe.

“We are a utility, and our role is to ensure that the systems are operating,” Jennings said.

During the Columbia recovery effort, 22,000 people and multiple agencies from the federal, state and local levels responded. “While the federal agencies had multi-million dollar gear, they couldn’t talk to each other. The local sheriff’s 200 ft. tower and radio system was completely overwhelmed and the federal VHF (very high frequency) system couldn’t connect to it,” Jennings said.

Jennings and his team deployed a mobile communications command center called the “COW” (communications-on-wheels) that quickly provided the critical link between NASA, local and federal systems. The COW, with its portable antenna and sophisticated gear, was able to link up 800 MHz systems, VHF, and more than five separate channels of emergency communication. The county also provided numerous additional base stations and radios to the shuttle recovery effort.

Flexibility was critical in the shuttle response. It is worth noting that Nacogdoches, Texas – the location of the shuttle recovery area – was well outside of Harris County and had significantly different terrain. The result, again in the words of NASA Director O’Keefe, was that “82,000 shuttle items were recovered, representing over 40 percent of the shuttle’s total weight.” NASA hailed the effort as one of the most successful disaster response efforts in the nation’s history.

LOOKING TO THE FUTURE

When speaking about specific security technologies, Jennings has high praise for new systems that rely on IP-based technologies to achieve plug-and-play interoperability.

“IP is the future. There are no ifs, ands or buts. That is where everyone is going.”

That said, Jennings notes that not all systems that are marketed as IP-based truly have that capability, and government buyers need to be cautious as they enter this new territory. Equally clear was the value of an interoperable response capability. According to Jennings, “the converged information utility approach is working great.”³⁴

GETTING STARTED

Michael Hamilton, CISO for the city of Seattle, has two main pieces of advice as government goes about its task of improving security: “making use of managed services” and “operationalizing security.” Managed services is, in general, a type of convergence.

“Many aspects of security are done best by a dedicated group of focused individuals,” Hamilton said, “and the free market leads to healthy competition in those areas.” Perhaps more importantly, Hamilton also notes that security cannot merely be a plan that sits on a shelf. To be effective, security must be “operationalized.”

For example, in the area of computer security, Hamilton reminds practitioners that, “Security people don’t run firewalls — network people do. Security people don’t manage patches — desktop people do. Each time there is an opportunity to create process and push security operations to groups that are specifically tooled up for operations, that opportunity should be seized.” To resolve this disconnect, it is highly recommended that security personnel work closely with IT managers and other operational teams when devising plans for the safety and security of their critical assets.

The Center for Digital Government reached out to thought leaders around the nation to gather their advice on getting started. To borrow a visual model from the Department of Homeland Security, here is what they said:

9

THINGS YOU MUST DO

1. Build relationships that go beyond siloes
2. Look for common, innovative solutions
3. Energize and empower your security staff
4. Understand the threats
5. Access your risk
6. Make use of managed services
7. Educate front line personnel
8. Develop coordinated response plans
9. “Operationalize” your plans — don’t just put them on a shelf

1

THINGS YOUR BOSS MUST DO

1. Reach out to engage other stakeholders — including other government entities and the public at large

1

THINGS THE FUNDING AUTHORITY MUST DO

1. Continue to define regional cooperation as a major priority for grant applications

CONCLUSION: ON KEEPING PEOPLE SAFE

“PLAN AS A TEAM, PRACTICE AS A TEAM, EQUIP AS A TEAM ... SO YOU CAN RESPOND AS A TEAM.”

Steve McCraw, director, Texas Homeland Security

This whitepaper set out to explore three areas:

- ✓ the rapid change and dynamic nature of the public safety threat matrix;
- ✓ the ways in which past approaches to safety and security are becoming outdated; and
- ✓ emerging models for integrated security that are meeting today's challenges.

The public safety threat matrix is indeed in a state of flux — with a multiplication in both the number and types of threats faced by public officials. It is not only crime or natural disasters that must dominate our planning, but crime *plus* natural disasters *plus* a wide ranging set of new threats. Response times must continue to shrink to meet the need of these new converged threats. While great progress has been made in improving cyber-security posture, much work remains to be done. Our flattening, interconnected world is transforming commerce for the good; it is also, regrettably, globalizing crime and the threats faced by our communities.

Past approaches were effective in their day, but they are typically “siloed” and insufficient to meet safety and security demands. Gone are the days when threats could reasonably be expected to come one at a time and citizen calls to 9-1-1 hotlines could be used as the primary mechanism for event correlation. Citizens call for a more integrated and faster response that puts critical assets in motion as soon as an emergency event occurs, thereby limiting damage to life and property.

Leading practitioners have developed effective ways to prioritize threats in a world where every type of event seems to have equal severity but resources are limited. In the words of Cory Ortigoza, “no plan survives first contact,” and the adaptability for dynamic re-prioritization is critical for success.

A new approach of integrated security networks — Security-over-IP — is setting a new standard for safety and security in real communities around the nation. This new model leverages existing investments and particular capabilities, while linking the coordination of response capabilities into a unified whole. Leading practitioners are making this happen while at the same time respecting citizen privacy and jurisdictional boundaries.

An integrated security network has five main components:

- ✓ distributed sensors to detect diverse hazards;
- ✓ a common data network to connect the disparate detection devices;
- ✓ integrated response systems — with event correlation capability — to make sense of the data;
- ✓ strong network security to prevent unauthorized access; and
- ✓ resilient infrastructure that can survive adverse conditions.

Real governments across the country are already seeing the benefits of this new approach in their jurisdictions. A converged approach to security is delivering the following benefits:

- ✓ more comprehensive pictures of an emergency situation;
- ✓ better capability for expansion and change over time;
- ✓ rapid re-tasking of resources in the event of changing threats; and
- ✓ better overall effectiveness and return-on-investment.

While the problem of ensuring safety and security has been around as long as government, we have seen that today's unique threat environment poses new and different challenges than we have seen in the past. The “bad guys” — be they criminals, terrorists or other malcontents — have incorporated technology into their plans; responders must do the same. Whether defending against routine crime, terrorist attacks, natural disasters or a pandemic public health crisis, an integrated approach that leverages a converged security network is critical to success. In the words of Texas Homeland Security Director Steve McCraw, “Plan as a team, practice as a team, equip as a team ... so you can respond as a team.”

FOOTNOTES

1. http://en.wikipedia.org/wiki/Code_of_Ur-Nammu
2. <http://www.nytimes.com/2007/04/17/us/17virginia.html>
3. http://www.vtreviewpanel.org/report/report/07_SUMMARY.pdf
4. http://www.vtreviewpanel.org/report/report/07_SUMMARY.pdf
5. Interview with Steve McCraw, Director of the Governor's Office for Homeland Security, state of Texas. January 19, 2009.
6. http://www.mlive.com/news/index.ssf/2008/12/mich_governors_mailroom_receiv.html
7. http://www.upi.com/Top_News/2008/12/12/FBI_White_powder_sent_to_30_governors/UPI-80231229116525/
8. <http://www.timesonline.co.uk/tol/news/world/europe/article2951485.ece>
9. <http://www.timesonline.co.uk/tol/news/world/europe/article2951485.ece>
10. "2008 Greek Riots – The Big Picture", Boston.com, http://www.boston.com/bigpicture/2008/12/2008_greek_riots.html
11. "Iceland Most Peaceful Nation; U.S. Ranked 97," ABC News, May 20, 2008, <http://abcnews.go.com/International/Story?id=4891902&page=1>
12. "Icelanders demand PM resign during violent protests," France 24, <http://www.france24.com/en/20081123-protests-geir-haarde-resignation-financial-crisis-iceland>
13. <http://blog.wired.com/defense/2008/12/the-gagdets-of.html>
14. Interview with Joseph Maida, former assistant attorney general for the state of Texas and Herat, Afghanistan, province team leader for the U.S. State Department, 2009.
15. Interview with Texas State CTO Brian Rawson and Deputy IT Security Director Walt Wilson, January 2009.
16. Interview with Dan Lohrmann, director of Michigan's Office of Enterprise Security and chief information security Officer, state of Michigan.
17. <http://www.securityfocus.com/brief/776>
18. <http://blog.wired.com/27bstroke6/2008/07/sf-city-charged.html>
19. Interview with Texas State CTO Brian Rawson and Deputy IT Security Director Walt Wilson, January 2009.
20. Identity Theft Resource Center. "2008 Breach List," courtesy of the Texas Department of Information Resources.
21. Interview with Mark Weatherford, director, Office of Information Security and Privacy Protection, state of California, January 2009.
22. Interview with Cory Ortigoza, former Congressional advisor on national security, January 2009.
23. Interview with Steve McCraw, director of the Governor's Office for Homeland Security, state of Texas. January 19, 2009.
24. Case Study, "Using IP technology to link dispatchers, emergency responders across jurisdictions," by Maj. Dean Hairston and Jeff Frazier, October 2007.
25. Interview with Steve McCraw, director of the Governor's Office for Homeland Security, state of Texas. January 19, 2009.
26. Book reference
27. <http://www.rand.org/>
28. Interview with Steve McCraw, director of the Governor's Office for Homeland Security, state of Texas. January 19, 2009.
29. Interview with Steve McCraw, Ddirector of the Governor's Office for Homeland Security, state of Texas. January 19, 2009.
30. Interview with Cory Ortigoza, former Congressional advisor on national security, January 2009.
31. Interview with Cory Ortigoza, former Congressional advisor on national security, January 2009.
32. Elaine Rundle, *Government Technology Magazine*, 2009. <http://www.govtech.com/gt/video/?id=614852>
33. http://en.wikipedia.org/wiki/Harris_County,_Texas#Geography
34. Interview with Steven Jennings, CIO for Harris County, Texas, February 13, 2009.

ACKNOWLEDGEMENTS:



John Miri, Senior Fellow at the Center for Digital Government

John Miri is the former Director of E-Government and Web Services at the state of Texas. He is an experienced government practitioner who has used technology to improve the safety and security of the people of his state. Miri launched the first official statewide Emergency Response Web Portal, which provided essential information for citizens, government and the media. He directed a public-private technology response to hurricanes Katrina and Rita, and also supervised the construction of Texas's first integrated Network and Security Operations Center (NSOC) in 2007. Miri directed TexasOnline.com, the state's official Web portal, which successfully defended against more than four million malicious intrusion attempts per year.

With the assistance of Paul W. Taylor, Ph.D., Chief Strategy Officer of the Center for Digital Government.



Cisco, (NASDAQ: CSCO), is the worldwide leader in networking that transforms how people connect, communicate and collaborate. For more information about Cisco's Safety and Security solutions, please go to www.cisco.com/go/govsafety



The Center for Digital Government, a division of e.Republic, Inc., is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

www.centerdigitalgov.com