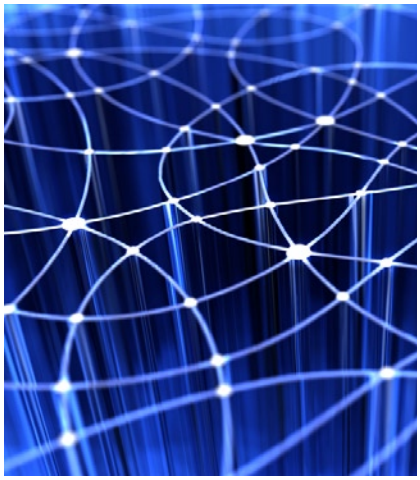


THE NEXT GENERATION OF SECURITY FOR NG9-1-1 SYSTEMS

The Challenge of Securing Public Safety Agencies

A white paper from FE/Kimball

JANUARY 2010 ©

An Expansion of Federal Engineering

L.R.Kimball℠

Combining Decades of LMR & PSAP Experience

HIGHLIGHTS

Authored by Jeremy Smith

Jeremy is an industry-recognized expert on securing 9-1-1 call centers and a Senior Network Security Consultant for FE/ Kimball. He has frequently been quoted by media outlets and is highly sought after as a guest speaker at 9-1-1 trade shows and conferences. He has written for publications like TechRepublic.com, *Public Safety IT Magazine*, *Emergency Number Professional Magazine*, *Security Pro VIP* and *Homeland Defense Journal*. Jeremy currently co-chairs the National Emergency Number Association's Security for Next-Generation 9-1-1 Working Group, which is developing cyber security standards (NG-SEC) for the public safety industry.)

The Next Generation of Security for NG9-1-1 Systems

The Challenge of Securing Public Safety Agencies

Next Generation 9-1-1 (NG9-1-1) brings about many long overdue improvements and changes in 9-1-1. The current 9-1-1 system is no longer capable of supporting the technology requirements of today's consumers. NG9-1-1 seeks to revolutionize and improve many of the underlying operational and technical components of the 9-1-1 system to improve its capabilities. By leveraging current technologies the public safety industry will be able to provide more comprehensive and robust service to the communities they are entrusted to protect. However, as with any evolution there are many challenges. One such challenge is ensuring that systems stay secure during and after the transition to NG9-1-1.

Historically, 9-1-1 call centers have been isolated, stand-alone networks. This closed-network architecture has helped protect the security of many of these call centers for many years. However, in NG9-1-1 call centers PSAPs, will be networked together, local public safety departments will be tied into regional agencies, and regions will be interconnected with federal agencies so that all emergency-related information can be shared at multiple levels to generate the most appropriate and swiftest response. This networking, while providing significant and notable benefits in our ability to respond to emergencies, can leave all the agencies within it much more exposed to viruses, denial-of-service attacks, hardware and software failures, intrusions by malicious hackers, data loss and system downtime than previously. Furthermore, 9-1-1 systems are particularly attractive targets for hackers and others who seek publicity for bringing down a highly visible network.

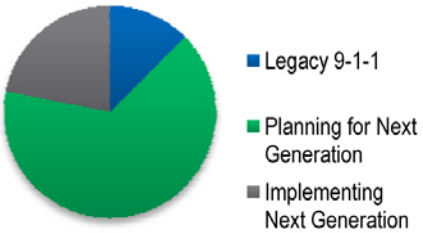
Any effective NG9-1-1 effort must include a cyber security component for it to be valuable in the long run. This whitepaper provides an overview of a recent survey conducted by FE/ Kimball, one of America's most prominent firms for developing and

HIGHLIGHTS

NG-SEC standards will apply to:

1. PSAPs
2. Telephone companies
3. Vendors
4. Content providers

More than 80 percent of survey respondents indicated that they were planning for or implementing NG9-1-1.



More than one in five agencies indicated that they were already implementing a NG9-1-1 system.

implementing emergency communications systems and a leader in securing public safety agencies. FE/Kimball surveyed public safety agencies on their cyber security concerns, incidents and approaches and is reporting our findings here along with several recommendations on how to address cyber security in a public safety agency.

READY—OR NOT?

Few would argue the overall advantages of NG9-1-1, and a few groups are working to protect the operations of the next generation of technology by employing cyber security measures. Cyber security entails keeping an organization's mission critical infrastructure or systems and their information safe, secure and available.

One of the groups at the forefront of cyber security is the National Emergency Number Association (NENA), which will soon be completing the development of security standards for NG9-1-1. These standards, referred to as NG-SEC, will apply to all 9-1-1 call centers, telephone companies, vendors, content providers and organizations implementing the most advanced networks and systems. The first comprehensive cyber security standards for the public safety industry, NG-SEC is an attempt to provide standards for ensuring the security of 9-1-1 during and after the transition to NG9-1-1 as well as raise the prominence of security within the public safety community. FE/Kimball, recently surveyed and received responses from approximately 100 directors and managers of local 9-1-1 systems; representatives of police, fire and sheriff's departments; and personnel from emergency management agencies to try to determine the extent of the new technology-related issues they were experiencing. The firm's research revealed:

- More than one in five of these agencies (22%) were already implementing a next generation 9-1-1 system.
- Two-thirds (66%) of the others were in the planning stages for NG9-1-1.

HIGHLIGHTS

The most common security issues among those we surveyed were virus infiltration and a failure that required restoring their computer system from backup.

When asked if they had experienced problems with cyber security over the past 24 months, 62% indicated that indeed they had. Moreover, these problems had resulted in outages or system downtime for well over half (54%) of the respondents. Among the most common issues were:

- Infiltration of viruses into their computer systems (18%)
- A failure that required the agency to restore its computer system from a backup source (17%)

In other instances, an employee had damaged computer systems or an outsider had tried to hack into the agency's system—and sometimes succeeded.

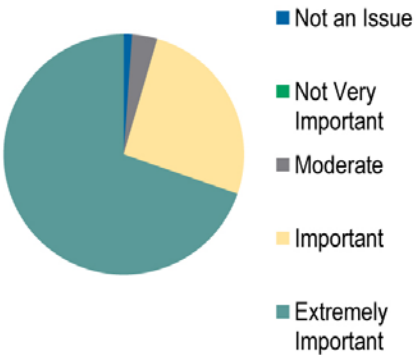
Anecdotally, the agencies reported a range of incidents that impacted their ability to deliver emergency assistance to the public. Among the accounts from individual departments were reports of:

- A virus infecting at least two computers because of the activity of an employee on the Internet
- A total radio outage resulting from the loss of a T1 line's connectivity, producing a chain of events that uncovered a software glitch in the trunk controllers
- A hacker entering the system and changing a hyperlink on the department's Web site to that of an adult site's address, despite the presence of firewalls, routers and security software
- A virus and spyware attack on a computer running the computer aided dispatch (CAD) system and numerous law enforcement software applications. This attack was the consequence of an employee using the Internet on that machine in contradiction to policy
- A CAD vendor logging in remotely and transmitting a virus to the system
- A virus on the network that targeted computers without the most recent security patches

HIGHLIGHTS

The majority of responders from our survey indicated that cyber security is an extremely critical issue.

More than 94 precent of respondents indicated that cyber security was an important or an extremely important issue.



Cyber security impacts legacy networks in addition to NG 9-1-1 networks.

- A virus received via e-mail from an unknown sender and another incorporated into a file
- Server software issues that unexpectedly rebooted the entire 9-1-1 system
- Accidental deletion of more than half of a user database by a third party administrator

All of these issues occurred despite the fact that 70% of the respondents indicated that they feel cyber security is an extremely important matter when migrating to NG9-1-1. Their biggest concern (56%) is system downtime, which can become a life-or-death situation for the community. A quarter of the respondents (25%) were most concerned about virus infections and 12% felt uneasy about being hacked.

One interesting finding was that more than 18% of respondents reported that a virus threatened the normal operation of their legacy 9-1-1 architecture. Cyber security needs to not only be addressed as a component of the NG9-1-1 transition, but also needs to be a consideration for closed network systems. 9-1-1 agencies need to begin planning, budgeting and securing funding for cyber security even before they've implemented NG9-1-1. Anti-virus software is an initial safeguard that can be implemented early on to help address cyber security for closed network systems.

The 9-1-1 department heads reported installing a number of cyber security safeguards:

- More than 96% have system backups
- 91% use firewalls (hardware or software that bars malicious traffic from networks)

Only 19%, however, employ penetration testing to determine the extent of their system's vulnerability.

Perhaps of even greater concern is that 89% have not yet begun budgeting for the new NENA NG-SEC security standards (in part because the standards were not ready as of the end of 2009). The result can be a rush to implement systems and networks

HIGHLIGHTS

Cyber security for mission critical applications must be handled differently because system downtime for installations and upgrades is simply not a solution.

complying with the new standards but with only a limited budget. Those factors can become a recipe for lax cyber security unless planning the protection of the new technology is integrated into the process from the start.

HOW TO INCREASE CYBER SECURITY IN A NG9-1-1 WORLD

Ensuring security for NG9-1-1 entails much more than simply finding the right software. It requires layers of defensive protection that integrate such precautions as:

- Antivirus software
- Security policies
- Vulnerability assessments
- Penetration testing
- Firewalls
- Hardened systems
- Patch management
- Secure remote access
- Encryption
- Backups of data and applications
- A security administrator
- Classification of data
- Risk management
- User awareness training
- and more

FE/Kimball Senior Network Security Consultant Jeremy Smith—who co-chairs the NENA NG9-1-1 standards committee with FE/Kimball Technical Specialist Gordon Vanauken, ENP—has noted that cyber security for mission critical applications must be handled differently because system downtime for installations and upgrades is simply not a solution.

HIGHLIGHTS

Organizations should start planning now for NENA's soon-to-be-released NG-SEC standards by budgeting now, including the right language in RFPs and thinking about incorporating security language into RFPs.

"For example," Smith explains, "a standard upgrade or security patch in the corporate world may be deployed such that those computers automatically reboot after installation of the patch. We can't be rebooting sporadically in a 9-1-1 system since that process may negatively impact an emergency call. FE/Kimball understands this kind of requirement because we have been providing solutions for 9-1-1 call centers for many years."

A comprehensive cyber security plan integrates many different and important measures. Ensuring that security is integrated into NG9-1-1 planning and implementation processes so that systems are constructed securely from their initial stages is crucial. Additional steps to increasing your security are:

- An NG-SEC compliance program
- Vulnerability assessments
- Security policies
- Managed services

By employing each of these approaches, described as follows, public safety agencies can help significantly increase their system's security.

NG-SEC COMPLIANCE PROGRAM

Organizations should start planning now for NENA's NG-SEC security standards. An NG-SEC readiness assessment is a good way to determine your compliance capabilities and begin to understand what it will take for you to comply. Experts can advise agencies of how to budget appropriately for the new standards, how standards might impact an upcoming procurement and how to ensure that the department includes the right language in it's Request for Proposal (RFP) for NG9-1-1 systems. Vendors building products with NG9-1-1 capabilities may want to ensure they will work and comply with the NG-SEC standards, and telecommunications providers may wish to understand how these standards affect their contracts and support models.

HIGHLIGHTS

The first step to determining if your system is compliant with NG-SEC standards is to conduct an NG-SEC readiness assessment to determine what vulnerabilities exist with your current networks and systems.

When the NG-SEC security standards are released, 9-1-1 agencies will be required to conduct audits internally that can be validated by third parties. Because NG9-1-1 networks are deployed in a variety of manners including both locally, regionally and nationally, the need to create organizations responsible for compliance auditing may occur. Until an organization is tasked with this responsibility, the requirements will fall into the hands of local 9-1-1 agencies to ensure the compliance with the NENA standard.

Achieving compliance with the standards will not only be important, but required. What steps can you take now to ensure you are working in the right direction?

- Conduct an NG-SEC readiness assessment to determine how far you have to go to achieve compliance. This affordable step will allow you to gain insight into your current vulnerabilities and help set the stage for full NG-SEC compliance program.
- Ensure that the equipment that you purchase is secure—this includes your customer premise equipment. Eventually, it is likely that vendors will need to validate their compliance with standards based on independent audits, but in the meantime, include security into your Requests for Proposals (RFPs) as well as your policies and network designs and contracts.
- If you are migrating an existing system begin to consider how you will bring it up to NG-SEC compliance.

VULNERABILITY ASSESSMENTS

The only way to determine the degree of vulnerability in a 9-1-1 system—or a vendor's claim regarding the security provided by its system—is to examine and test it. A vulnerability assessment is an affordable way to baseline systems and processes and where gaps exist.

Assess security vulnerabilities using advanced software tools and highly trained security experts. The process should involve a thorough and comprehensive examination of networks and systems. It can be done by plugging specialized equipment into the networks and conducting an unobtrusive scan. Weaknesses, vulnerabilities and areas that cyber criminals might try to exploit will

HIGHLIGHTS

A vulnerability assessment will provide you with a baseline evaluation of your network and systems. It should be conducted periodically to ensure that new threats and major system changes are accounted for.

be identified. It can be conducted on the entire network, a part of it or only a specific system or application.

Once a vulnerability assessment is conducted, the findings should be summarized in a written and verbal report that explains the findings and associated risks in terms that relate to the agency's specific goals and objectives. This document can help to mitigate the agency's risk and strategies can be taken to address vulnerabilities and bring networks and systems into a fully secure state.

Assessing the vulnerability of 9-1-1 networks and systems provide agencies with a baseline evaluation of a network and systems and should be conducted periodically to ensure that the highest level of security is maintained. As new threats emerge or after major systems changes or upgrades, vulnerability assessments can be useful tools in understanding where new points of risk exist and can help ensure that systems are in compliance with policies and standards.

VoIP SECURITY

Voice-over-IP (VoIP) phone networks can be just as vulnerable to security threats as any other computerized network that is based on the flow of digital data. For example, how will organization's deal with a Denial of Service (DoS) attack in an NG9-1-1 environment? Develop a comprehensive plan for identifying and mitigating VoIP security risks in a manner consistent with overall security plans and policies.

SECURITY POLICIES

The security of a system depends equally on people, products and policies. Security policies are as crucial to an organization's safety as any piece of equipment or the personnel who use the system. A security policy documents specific goals and objectives regarding a security program and helps define the kinds of behaviors that are allowed or not allowed. For example, an acceptable use policy

HIGHLIGHTS

Employing managed services offering will help a 9-1-1 agency offload the maintenance and monitoring of security software or solutions. This includes new Microsoft security patches, managing antivirus updated every day and managing firewalls.

specifies the kinds of things can be done with an organization's computer systems and what cannot (like inappropriate use of the Internet, playing games, personal use of the computer while on duty, etc). Policies also can be used to provide clear requirements for how systems should be configured or hardened (network security policy) or furnish parameters for hiring practices and background checks. Experts can help the agency develop these policies as well as build incident response plans, business continuity plans, and policies for data classification, data backup, outsourcing, passwords, remote access and other actions.

MANAGED SECURITY SERVICES

Many organizations struggle with how to manage their security software and solutions on a daily, weekly and monthly schedule. Examples of such efforts include pushing out new Microsoft security patches, managing antivirus updates each day and managing firewalls. Managed services offerings allow organizations to completely offload the maintenance and monitoring of security software or solutions to an expert managed services team. Additionally, it can also significantly enhance your ability to achieve NG-SEC compliance and more importantly become and stay secure while keeping costs down. Many organizations continue to turn to managed services solutions to improve their security without hiring full time security staff.

HIGHLIGHTS

Use this checklist as you transition to NG9-1-1 to ensure that cyber security is accounted for.

WHAT YOU SHOULD BE DOING NOW

Before moving further with a NG9-1-1 plan, take the following steps:

- ✓ Include cyber security as a required component throughout your plan.
- ✓ NG-SEC readiness assessments are an affordable and great way to determine how much work is ahead of you.
- ✓ Budget for cyber security. It's much more economical to do so at the beginning of the project than to pay the price for technology crises later on.
- ✓ Ensure that all equipment purchases are secure by working with an expert team to evaluate them.
- ✓ Be certain that your emergency system network requires entities connecting to it to adhere to NG-SEC standards so that you maintain security throughout and across networks.
- ✓ Make NG-SEC standards part of any RFPs that your agency issues.
- ✓ Seek outside help if needed.

With forethought to protecting NG9-1-1 systems, public safety agencies can stay secure and available for carrying out their mission of protecting their communities.