WINBOURNE™
CONSULTING, LLC

January 2021 Newsletter

January 2021

Cyber Security - An Important Initiative for 2021

As public safety agencies move towards utilizing cloud-based NG9-1-1 technology for everything from data storage to CAD, Mobile, and RMS, cyber security becomes an even greater concern. Winbourne has reached out to our cyber security partner **SecuLore Solutions**, **LLC** to provide information on some of the processes, procedures and "things" agencies should consider in developing a plan of action to implement a cyber security action plan. These recommendations are applicable in defending against cyberattacks in both a traditional and cloud-based environment.

- **Identify a Chief Information Security Officer (CISO).** One of the first things an agency should do is to identify a Chief Information Security Officer (CISO), an individual whose responsibility is to manage information and network security for the organization. The CISO is the individual for improving and maintain the cybersecurity posture for all the departments within the jurisdiction.

- **Create A Written Cyber Response Plan.** A written cyber security response plan is key and needs to be tested at least quarterly to ensure recovery from backups. The backups should be Spot-checked for consistency and viability to ensure that saved correctly. Quarterly testing of backups by using a backup PSAP is one of the the most effective ways of accomplishing this task. The plan should include affirmative coverage cyber insurance that would cover costs of 3rd party assistance to aid with recovery. If using a 3rd party cyber-expertise vendor it is best to enure that the vendor is approved by your insurance provider.

- **Remove Barriers to Implementation**. A primary responsibility for the CISO is to ensure there are no external barriers to the implementation of mitigation techniques due to a variety of factors including local governance that may limit the ECC's ability to perform one or more of the identified cyber mitigation functions. There a number of components that could affect the agency's ability to perform some of its mitigation factions that need to be identified and resolved. These components can typically include issues such as governance e.g., County or State level management of the IP infrastructure used by the ECC, or regulations or laws that preclude the agency's ability to perform the mitigation tasks such as the the Criminal Justice Information Services password rules.

- **Implement Continuous Cyber Monitoring And Vulnerability Assessments.** This is the single-most comprehensive solution for cyber-defense. These assessments should be in practice before using an IP-based technology for mission critical emergency services. If the agency is already at that stage of evolution and continuous monitoring and vulnerability assessments are not in place, the should be implemented as

Winbourne Consulting **offers a full range of public safety services, including strategic planning, systems integration, specifications development, solution acquisition, and implementation project management and quality assurance**.

soon as possible. The vulnerability assessments should occur at a minimum of every 90 days across the whole of the infrastructure. However, if the type of cyber monitoring provides weekly reports and regular external analysis, then vulnerability assessments could instead be done annually.

- **Acquire the best firewall Possible.** It is generally a best practice to acquire the best firewall possible, use network segmentation and put sensitive information behind additional firewalls; and limit user privileges to only what is needed to accomplish specific job duties. Remote access should be protected by using a secure methodology that is updated to the latest version and meets or exceeds the minimum standard (NIST 800-53) of password creation and storage, and utilizes a multifactor authentication methodology.

- **Provide cyber-safe methods for staff members to perform personal tasks** that are inherently necessary in the course of a telecommunicator's work responsibilities. These important incidental mitigation techniques for non-intentional impacts include a wide variety of tools such as 1) providing individual separate USB charging stations or equivalent methods (data blocker dongles) to charge personal phones/tablets, 2) establishing a guest network (either managed or outside of the emergency services network) to accommodate Bring Your Own Device (BYOD) usage, 3) disable the local USB ports (at a user privilege level if possible), etc.

Backups

- **Create Discrete Backups.** Implement a program of three (3) backups on two (2) different forms of media storage (such as cloud, tape, external drive, flash drive) that can be connected on demand. These backups should not be allowed to be connected until needed. At least one of the backups must be stored offsite, and geographically & logically separated from the others.

- **Ensure That a Full Backup Is Being Accomplished.** Auto-syncing cloud services do not constitute a full backup, even though they are often marketed as such to private individuals and even to large enterprises. These services replicate a copy of data locally and via a cloud service. It is true that these services do protect from one vulnerability, which is the loss of data through loss of a device, such as if the device is destroyed or experiences hardware failure. These services also allow for rapid restoration, because even if an end-user device is destroyed, the data can simply be accessed and re-provisioned onto a replacement device.

- **Protect the Agency from Data Compromise**. However, these services do not protect from other forms of data compromise. For example, if data is altered maliciously, those alterations will be replicated in the cloud. If data is corrupted, the corruption will be replicated in the cloud. Or if information is simply deleted, whether by accident or by a malicious user, the remote copy will be lost as well; as the cloud service will replicate any local changes, as it is designed to do, which in this case would be to delete the copy of the file on the cloud—deleting the "backup".

- **Implement a Comprehensive Backup System.** Accordingly, cloud-syncing services should not be considered a comprehensive form of backup, and do not necessarily satisfy the recommendation above to provision three backups of any critical data.

Our Areas of Expertise **encompass all segments of Public Safety, including:**

● **PSAP Consolidation**
● **NG911 Strategic Planning and Implementation**
● **Public Safety Communications and Telephony**
● **Public Safety Applications and Systems Requirements and Implementation Support**
● **Mission Critical Facilities Design and Fit-Out**
● **311 Call Centers and Implementation**
● **PSAP Staffing and Operations Analysis**

Winbourne Consulting and its partner SecuLore Solutions can offer assistance with all aspects of cyber security from assessments, to planning to implementation. For additional information contact Winbourne Consulting at info@w-llc.com.

Our thanks to **Tom Breen, Cybersecurity Liaison, SecuLore Solutions**, LLC for his contribution to this article.

Winbourne Happenings

Arlington County, Virginia Fire Department successfully completed the migration to the ImageTrend Fire Records Management System in December. Winbourne Consulting provided Project Management and Subject Matter Expertise to the Department, to include strategic planning, vendor acquisition support, and implementation management. The project successfully integrated the Department's National Fire Incident Reporting and Emergency Medical Services Electronic Patient Care Reporting System in one common platform.

On January 13, 2020 the Arlington County, VA Emergency Communications Center (ECC) demonstrated remote dispatching and supervision in addition to its previously deployed remote 9-1-1 call taking capability. During the launch event a dispatcher and a supervisor worked from their respective homes connected to the ECC's systems via broadband and wireless networks.
One of the hallmarks of the deployment is ensuring that dispatchers have a fully functional solution available to them that mirrors all the radio capabilities they would have present at the ECC - including multiple talk groups, access to the instant recall recorder, and ability to respond to an emergency activation.

This new capability builds upon the shared Next-Generation 9-1-1 call handling system the County installed in 2019 with the City of Alexandria. **Winbourne Consulting provided both jurisdictions with project management services throughout that initiative including governance agreements, requirements definition, RFP development and system implementation.** We continue to assist Arlington County develop their long-term strategy for a permanent, sustainable remote operations capability.

For additional information visit: **https://newsroom.arlingtonva.us/release/arlington-emergency-communications-center-leads-nation-in-remote-call-taking-dispatching-supervision/**

In January 2021, Winbourne Consulting completed a two-year engagement with the Chula Vista Police Department in support of their Unmanned Aircraft System (UAS). Chula Vista developed cutting edge drone

Clients **include city, county, state, and federal agencies located throughout the United States and the world, as well as countries in Europe, the Middle East, Asia, the Caribbean, and South America.**

use in public safety and Winbourne was contracted to assist with strategic & operational support. Primary tasks accomplished during our engagement included:

1. Development of the UAS-DFR (Drone-as-first-responder) Best Practice Reference Guide.
2. Tracking and management of the large number of vendors who sought an audience with Chula Vista. We helped maintain alignment between the vendors offerings and the department goals and objectives.
3. Development of an updated Policy & Procedure section.
4. Development of the UAS Program Strategic Plan.
5. Development of the UAS Program Mission-Vision-Goals-Objectives document. This is a living document intended to help keep the UAS program aligned with the Strategic Plan.
6. Supported City Procurement in the development of an RFP soliciting program support and pilot services for the UAS program.

Winbourne Consulting recently completed its annual customer satisfaction survey of our current and past customers. Winbourne is pleased to report that we have received an overall customer satisfaction score of 97%. Additionally, all our survey respondents said that they would engage Winbourne Consulting for future assignments and would recommend Winbourne's services to other agencies.
"Winbourne takes pride in maintaining our 97% percent satisfaction rating over these years. It is a reflection of our primary corporate focus of truly understanding and meeting the needs of our clients.", Andrew Reece, Winbourne Consulting C.E.O.

Industry Events

NENA Cancels In-Person 2021 9-1-1 Goes to Washington Conference

On October 27, NENA announced that it has cancelled its upcoming 9-1-1 Goes to Washington event, originally planned for February '21, due to the ongoing public-health and safety concerns related to the coronavirus (COVID-19) pandemic. NENA is exploring the possibility of hosting a virtual 9-1-1 Goes to Washington in February of 2021.

Articles of Interest

How Assistive AI Improves Emergency Response

Every city faces public safety emergencies, from routine traffic incidents to crime, extreme weather and more. Speed, efficiency and effectiveness are the linchpin of emergency response during these situations, and delays or misinformation during such events can be catastrophic.

The unsung heroes at these moments of distress are the personnel manning 911 call centers. Call-takers are the first line of defense, connecting residents with the appropriate resources as expeditiously as possible. Dispatchers similarly need as much assistance as possible from the tools at their disposal to determine the correct response and direct field personnel accordingly.

For more information about our services and solutions, visit our website at:

www.winbourneconsulting.com

To read the full article visit:
https://gcn.com/articles/2020/11/04/assistive-ai-public-safety.aspx?admgarea=TC_PublicSafety

RadioResource MissionCritical COMMUNICATIONS | RadioResource INTERNATIONAL

NENA, CIS Partner on Cybersecurity for NG 9-1-1 Systems

In an effort to develop and promote cybersecurity awareness and resources within the 9-1-1 community, the National Emergency Number Association (NENA) and the Center for Internet Security (CIS) adopted a memorandum of understanding (MoU) to guide joint initiatives and encourage best practices between the two organizations.

"As we continue to lead the transition from legacy 9-1-1 to NG 9-1-1 technologies, it is imperative that we elevate 9-1-1 professionals' knowledge of cybersecurity issues," said NENA President Gary Bell, ENP. "NENA is excited to deepen our collaboration with CIS and we are confident this partnership will help improve public safety in every community."
The full story can be viewed at:
https://www.rrmediagroup.com/News/NewsDetails/NewsID/20400

URGENT COMMUNICATIONS

IoT Security Trends, 2021: COVID-19 Casts A Long Shadow

In 2020, COVID-19 left few stones unturned with its upending impact on health, society, the economy and technology itself.

Internet of Things (IoT) security was no exception. The novel coronavirus, which causes COVID-19 disease, brought new security issues to the fore, and these issues stand to ricochet through 2021 and beyond.

As many activities became remote, digital and more connected (think digital health, videoconferencing and facility remote monitoring), threats also became prevalent. Many of these IoT security threats only broadened the surface area for attacks and moved targets from centralized locations (the office) to the edge of the network.

"We saw a push to remote work, which certainly changed the threat landscape," said Merritt Maxim, vice president and research director at Forrester Research. Examples include "trying to go after users through more sophisticated phishing attacks. Users [were] at home … [and] not as on guard as when they were in the office," he said. "COVID-related threats are going to persist into this year and probably in the next and, in some cases, could be permanent."

As IoT devices proliferate – and there may be some 21.5 billion devices by 2025 – it becomes even more critical to secure IoT environments and prevent breaches.
To read the complete article visit: https://urgentcomm.com/2021/01/26/iot-security-trends-2021-covid-19-casts-a-long-shadow/

Verizon Calls On Industry To Provide 'True Interoperability' To First-Responder Community

Telecommunications giant Verizon announced that it is working to create a broad industry coalition that would address the longstanding public-safety communications issue of “true interoperability” between first-responder entities, according to a Verizon executive.

Andres Irlando—a Verizon senior vice president and president of the carrier’s Public Sector and Verizon Connect unit—said the company “has been working very aggressively” on interoperability, which has been cited by first-responder customers and the Verizon First Responder Advisory Council as a priority for public safety.

The full story can be viewed at:
https://urgentcomm.com/2021/01/25/verizon-calls-on-industry-to-provide-true-interoperability-to-first-responder-community/

Look us up on LinkedIn

https://www.linkedin.com/company/winbourne-consulting-llc?trk=biz-companies-cym

We Are Interested in Your Thoughts on the Above Topics.
To share them with us, please:

Email us at: info@w-llc.com
Or
Twitter us at https://twitter.com/winbournellc

For more information about our services and solutions, visit our website at:
www.winbourneconsulting.com

Look us up on LinkedIn
https://www.linkedin.com/company/winbourne-consulting-llc?trk=biz-companies-cym