



## February 2022

February 2022

**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.**

### **Where Does Your Agency Stand When It Comes to Cyber Security?**

Cyberattacks have been in the forefront of news stories, with hundreds of attacks reported against companies and governments across the country. Most of these attacks originate in China and Russia making it an international crisis. The frequency of cyberattacks, including malware, ransomware and theft of data has escalated the need for Public Safety agencies to prepare and manage a robust cyber security strategy.

The cyber threat is even more acute with many Public Safety agencies implementing remote work options for employees.

In a January 22 article in the American City and Article, the current study by SolarWinds showed that cyber security threats are increasing, but the public sector's ability to detect and deter these threats has not kept pace with the number and increasing sophistication of these threats.

Our January 2021 newsletter lead article discussed some of the various aspects related to cyber security and discussed a number of steps that can be taken to defend against cyber threats. **A copy of that article can be found here:** <https://www.w-llc.com/2021/01/>

### **Cyber Security Assessments**

When building cyber security defenses, the first step is to perform an assessment of the current system.

The assessment should include the creation of stated goals and objectives, which should include preparing, conducting, and analyzing results to gauge risk. The National Institute of Standards and Technology (NIST) states that the Assessment results should provide the agency with the following analyses:

- Effectiveness of implemented systems
- Quality of the risk management processes
- Information about the security, privacy strengths and weaknesses of the systems
- Review of current cyber security mitigation for staff members

Each year NIST publishes an updated publication called "Assessing Security and Privacy Controls in Information Systems and Organizations". While the publication is lengthy, it is designed to be used by a wide range of public sector agencies in developing an assessment plan. **The publication is free and can be found at:** [https://tsapps.nist.gov/publication/get\\_pdf.cfm?pub\\_id=933932](https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=933932).

### **Cyber Security Programs**

The creation of a cyber security program is the second step in dealing with cyber security threats. The goals of a cyber security program would be to:

## Winbourne Areas of Expertise:

- 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

- Reduce the likelihood of a damaging cyber incident; this includes preventing devices from connecting to malicious sites and scanning for security weaknesses and vulnerabilities, etc.
- Detect malicious activity quickly, including by deploying network intrusion detection and prevention, undertaking penetration testing, and improving endpoint detections
- Respond effectively to confirmed incidents, including through collection and analysis of malware and other artifacts
- Maximize resilience, including by automating system backups and enhancing threat modeling
- Provide cyber safe methods for staff members to perform personal tasks

Cybersecurity and Infrastructure Security Agency (CISA) recommends certain measures that should be taken to establish a foundational cyber security program such as:

- Fix the known exploited security flaws in software
- Implement multifactor authentication
- Stop bad practices that are exceptionally risky
- Reduce Internet attack surfaces and get your Stuff off Search
- Sign up for CISA's cyber hygiene vulnerability scanning

For additional information and a list of the tools, visit the CISA website.

<https://www.cisa.gov/news/2022/02/18/cisa-launches-new-catalog-free-public-and-private-sector-cybersecurity-services>

**Winbourne Consulting** has assisted numerous clients in assessing various aspects of their operations including cyber threat protection. For additional information contact <mailto:info@w-llc.com>

---

## Cyber Security Articles

### Small Cities Worry Cybersecurity Money Won't Reach Them

Even though small, under-resourced municipalities often fall victim to cyberattacks, many don't have the resources to put together a proposal for a share of the \$1 billion in federal cybersecurity grants available through the new infrastructure law.

To view the complete article visit: <https://gcn.com/cybersecurity/2022/01/small-cities-worry-cybersecurity-money-wont-reach-them/360944/>

### Report: Cyber Threats Are on the Rise While Public Defense Measures Lag

Technology is evolving and so are the online threats faced by local governments. But faced with these increased criminal threats, defensive measures aren't keeping pace. For the first time in five years, an annual report from SolarWinds cites external threats as the public sector's greatest cybersecurity concern.

"While IT security threats have increased—primarily from the general hacking community and foreign governments—the ability to detect and remediate such threats has not increased at the same rate, leaving public sector organizations

**Our 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.**

vulnerable,” said Brandon Shopp, group vice president of product strategy at SolarWinds in a statement.

To view the complete article visit:

<https://www.americancityandcounty.com/2022/01/11/report-cyber-threats-are-on-the-rise-while-public-defense-measures-lag/>

### **IoT Devices Most Vulnerable To Internal Security Threats**

A new study has found internal employees are the biggest security threat to a company, with IoT devices being the most vulnerable.

Cybersecurity threats from the inside, whether it's from contractors or employees, continue to be a growing worldwide concern, with vulnerable IoT devices at the greatest risk for data losses.

Those insider threats have increased in both frequency and cost over the past two years, according to the Ponemon Institute's Proofpoint's 2022 Cost of Insider Threats Global Report.

The 2022 report includes survey responses from more than 1,000 IT professionals worldwide who experienced a recent cybersecurity incident due to an insider threat.

To view the complete article visit: <https://urgentcomm.com/2022/02/24/iot-devices-most-vulnerable-to-internal-security-threats/>

### **Cybercriminals Carried Out a Record Number of Ransomware Attacks Last Year; Experts Expect More In 2022**

It might be a different year, but old threats linger—especially in cyberspace. An advisory covering the current cyberthreat situation issued by federal agencies and international partners Wednesday outlines a growing threat posed by ransomware that's expected to continue through 2022.

“Cybercriminals are increasingly gaining access to networks via phishing, stolen remote desktop protocols, credentials or brute force, and exploiting software vulnerabilities,” the advisory says. Over the last year, especially, “The market for ransomware became increasingly ‘professional’ and there has been an increase in cybercriminal services-for-hire.”

To view the complete article visit:

<https://www.americancityandcounty.com/2022/02/09/cybercriminals-carried-out-a-record-number-of-ransomware-attacks-last-year-experts-expect-more-in-2022/>

---

## **Winbourne Happenings**



**Winbourne Consulting is assisting the City of Virginia Beach with the implementation of CentralSquare's CAD-to-CAD product.** This is part of a regional CAD-to-CAD project involving the cities of: Chesapeake, Suffolk, Portsmouth, and Norfolk.



**Winbourne Consulting was awarded the contract to assist the Southeast NE 911 Board** with the area PSAP's migration to the new Nebraska NG911 system including procurement of compatible call handling equipment.

---

## Industry Events

### 9-I-I GOES TO WASHINGTON

**\*\*NEW DATE\*\* March 15-18**

*The health and safety of NENA event attendees is a top priority, and, as such, we have moved #NENAGTW to March. The new dates are March 15-18. Current registrants received an email on Friday, January 21 to confirm their attendance on the new dates. Hotel reservations for the original February dates were cancelled automatically. Attendees should have rebooked housing for the event (the lodging link went live on or before February 1).*

**911 Goes to Washington** brings together hundreds of 911 professionals from around the country with policy leaders in our nation's capital to explore and discuss today's most pressing 911 and emergency communications issues. 911 Goes to Washington is the only event where you can learn about the policy challenges facing public safety and take immediate action to address them through dialog with your elected and appointed officials.

For additional information, visit: <https://www.nena.org/page/gtw>



**The IACP Technology Conference** is the premier professional event dedicated to discussing technology in law enforcement. Attendees should expect quality training, professional development, and networking covering a broad array of new and emerging technologies.

For additional information, visit: <https://www.theiacp.org/tech-conference>

---

## Articles of Interest



### **Report Finds Emergency Responders Need More Tools, Resources to Public-Safety Broadband Applications and Benefits**

Every day, the news serves as a near constant reminder of the emergency issues plaguing the world, from tornadoes in the Midwest to flooding in Western Canada to disasters requiring the swift dispatch and coordination of multiple response units and divisions.

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

[www.winbourneconsulting.com](http://www.winbourneconsulting.com)

Look us up on  
LinkedIn

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

Where timing and proper, clear communication is a matter of life or death, infrastructure and technology become the backbone of emergency response, especially in more remote and isolated areas. In our highly digital world with a massive amount of mobile phones, internet of things (IoT) devices, sensors through LTE/5G networks and satellites, these advances are, thankfully, also benefiting public safety.

The full article can be viewed at:

<https://www.rrmediagroup.com/Features/FeaturesDetails/FID/1099>

### **APCO Standard on Operational Overload Receives ANSI Final Approval**

The Association of Public-Safety Communications Officials (APCO) International received final approval from the American National Standards Institute (ANSI) on for a newly created American National Standard (ANS) titled "Managing Operational Overload in the Emergency Communications Center (ECCs)."

In today's environment, ECCs regularly experience situations where workload has the potential to overwhelm personnel. This standard provides ECCs with best practices for planning, mitigating and handling operational overload.

To read the complete article visit:

<https://www.rrmediagroup.com/News/NewsDetails/NewsID/21348>



### **Rosenworcel Proposes Using Spectrum-Auction Proceeds To Fund NG911 Deployments**

FCC Chairwoman Jessica Rosenworcel this week proposed that future auction proceeds be used to fund the technological migration of U.S. public-safety answering points (PSAPs) from legacy systems to IP-based next-generation 911 (NG911) platforms.

Rosenworcel unveiled her idea during an event organized in Washington, D.C.—organized by the Public Safety Broadband Technology Association—celebrating the 10th anniversary of the FirstNet Authority being created to build a nationwide public-safety broadband network (NPSBN). A key player in the push for FirstNet while serving as counsel to the Senate Commerce Committee a decade ago, Rosenworcel cited numerous parallels between the FirstNet initiative and the NG911 transition.

To read the complete article visit: <https://urgentcomm.com/2022/02/25/rosenworcel-proposes-using-spectrum-auction-proceeds-to-fund-ng911-deployments/>

### **FirstNet Users Enjoy Largest Coverage Footprint In The U.S., AT&T Says**

FirstNet subscribers have access to the wireless network with the largest coverage footprint in the United States by more than 50,000 square miles, AT&T stated this week as part of press announcement released on the 10th anniversary of the FirstNet Authority being created.

Jason Porter, president of AT&T's public-sector and FirstNet business units, said AT&T—the FirstNet Authority's contractor building the nationwide public-safety broadband network (NPSBN)—has spent more than \$130 billion on wireless infrastructure and spectrum in the five years since being awarded the FirstNet contract in March 2017.

The full article can be viewed at: <https://urgentcomm.com/2022/02/24/firstnet-users-enjoy-largest-coverage-footprint-in-the-u-s-att-says/>

---



**We Are Interested in Your Thoughts on the Above Topics.**

**To share them with us, please:**

**Email: [info@w-llc.com](mailto:info@w-llc.com)**

**or**

**Twitter: <https://twitter.com/winbournellc>**

---

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

**[www.winbourneconsulting.com](http://www.winbourneconsulting.com)**