LAW ENFORCEMENT | PUBLIC SAFETY SEMINAR

OCTOBER 30, 2024
Minneapolis Marriott Northwest

14TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY SUMMIT
Security solutions through collaboration.™

The Cyber Security Summit is excited to present the first of its kind Law Enforcement Seminar. From threats to breaches, ours is a community of professionals who focus on protecting what matters most for our agencies, our families, and our communities. This is a day designed for law enforcement and criminal justice crimefighters as we tackle the technical topics that will make a difference.

Cyber Threats: Calling All Units

The last ten years have seen significant investments in community oriented policing, active shooter response, and sex trafficking. Priorities point today to an explosion in cybercrime, with more victims, greater costs, and ever-sophisticated methods. By leveraging video and audio deep fakes with the power of social engineering and human vulnerabilities, criminals are on a roll. Law Enforcement and Public Safety personnel are faced with new tactics, multi-faceted methods, and the need for additional training and tools to take it all on. Join the Cyber Security Summit Law Enforcement | Public Safety Seminar on **Wednesday, October 30** for a critical day of content, designed by and for the response ecosystem of professionals at the intersection of cyber and crime.

Who should attend

Law Enforcement Officers, forensic techs, intel analysts, dispatch, fire and military personnel (POST credit pending).

Content created by

Developed with a collective 250+ years' experience from the Minnesota Bureau of Criminal Apprehension, DHS Homeland Security Investigations, FBI, CISA, Minnesota State Patrol, Hennepin and Ramsey County Sheriff's Offices, Minnesota Military Cyber Professionals Association, Jewish Community Relations Council of Minnesota and the Dakotas, Association of Threat Assessment Professionals chapter and others.

Register at cybersecuritysummit.org
$299 registration fee includes lunch.

Topics

Cyber Incident Intel: How Common are These, Really?
View evolving business models, crime types and trends through local, national, and global lenses.

Ransomware Response: Tactical and Practical
A look at ten years of ransomware response: where we've improved, and what to prepare for.

Reporting Requirements for Frauds, Scams, Sextortion and Deep Fakes
The despair, losses and shame inflicted through cybercrime have affected every community. Learn what to report, how to report, and when to report.

Got Your Six: State and Federal Support Capabilities
Federal, state, and military partners provide robust support programs and forensic capabilities: sharing intelligence, tips to protect critical infrastructure, and a collective response when prevention fails.

Cyber Threat Prevention - Community Education Cuts
Crime Outreach programs make a difference and education results in fewer victims. Two fraud fighters tell stories relentlessly and have seen a reduction in incidents for the over-50 demographic.

Bad Actor Lineup: Domestic and Foreign Threats
What you can and can't do is governed by different laws, statutes, and jurisdictional interpretations. Domestic enforcement is easier than international, and this session provides clarity to a known gray area.

AI, Deep Fakes, Scams and Solicitations
Deep fakes make scams scarier, as AI augments a criminal's ability to gain trust and exploit people for monetary gain or worse.

Hostage Hotwash: School System Shutdown
This ransomware tale is a true bombshell. A first-person perspective starts when a large, public school system comes to a halt. All the chapters - from initial panic, the identification of internal, external, state and federal response resources, technical elements, law enforcement collaboration, recovery mode, media matters and community impacts – wrapped up with 'lessons learned' tips for avoidance.