

InfraGard National Members Alliance is proud to partner with RSA Conference™ to bring you an exclusive two-day training opportunity.

Secure your spot today and join us in San Francisco for *Cyber Defenders: Guardians of Critical Infrastructure.*

REGISTER NOW

Training Overview:	**Cyber Defenders: Guardians of Critical Infrastructure** Our nation is constantly at war in the cyber realm. From cyber criminals to highly sophisticated foreign adversaries, the relentless assaults on the private sector pose the single greatest threat to our national security, economic interests, and critical infrastructure – the foundation of American life. This two-day executive training session will arm cybersecurity professionals and non-technical executives alike with the knowledge, tools and resources to become cyber defenders and prevail on this vital warfront.
Learning Objectives:	Attendees will gain an understanding of today's threat actors with briefings from the FBI Cyber Division and other government agencies; learn the rules of engagement with an exploration of emerging cyber laws and legal trends shaping the regulatory environment; understand foreign adversaries and the tactics, techniques, and procedures (TTPs) they use to gain information with briefings from the FBI Counterintelligence Division; learn how to leverage cyber threat intelligence; and participate in how-to sessions with private sector experts on developing 'reasonable security' and insider threat programs.
Sessions:	Session I: Heroes and Villains: An FBI Threat Briefing Session II: The Rules of Engagement: Emerging Cyber Laws and 'Reasonable Security Session III: Threat Hunters: Cyber Intelligence for CIKR Session IV: Under Attack: Foreign Adversaries and the Threat to National Security Session V: Hunting the Enemy Within: Insights from a Mature Insider Threat Program Session VI: The Moment of Boom: Attacks on American Soil Session VII: The End Game: Putting Your Cyber Investigation on Trial Session VIII: Harnessing Your Superpowers: The Business of Cyber
Dates:	Sunday, April 23 from 9 am – 5 pm | Monday, April 24 from 9 am – 5 pm
Venue:	RSA Conference, Moscone Center, 747 Howard St., San Francisco, CA 94103
Registration:	https://www.rsaconference.com/usa/networking/tutorials-and-trainings
Cost:	$2000 for this two-day executive training session.

Session I: Heroes and Villains: An FBI Threat Briefing

The FBI San Francisco Field Office will provide an overview of the cyber actors dominating the current threat landscape, from cyber criminals to foreign adversaries. Hear directly from the FBI about timely risks and threats to the private sector and the FBI's role in investigating and prosecuting cyber crimes.

Session II: The Rules of Engagement: Emerging Cyber Laws and "Reasonable Security"

Leading cybersecurity attorneys and in-house counsel will discuss emerging cyber laws and legal trends, including major changes driven by new federal and state laws and regulations that require organizations to develop comprehensive cyber programs. This session will explore the often-amorphous concept of "reasonable security" and what technical, administrative and procedural safeguards that concept includes. Fedaeral and state laws, including the California Consumer Privacy Act (CCPA) require companies to implement reasonable security controls to protect personal information and other sensitive data. Hear about the current state of laws and gain guidance on the considerations and cornerstones of a reasonable security program.

Session III: Threat Hunters: Cyber Intelligence for CIKR

Geopolitical events in Eastern Europe beginning in February 2022 led the U.S. Cybersecurity and Infrastructure Security Agency (CISA) to anticipate cyberattacks extending to the homeland. CISA's Shields Up campaign turned U.S. information technology workers into cyber threat hunters, regardless of their existing cybersecurity savvy. One year into the conflict, these workers —across all 16 Department of Homeland Security-designated critical infrastructure and key resources (CIKR) sectors— face cyber vigilance fatigue. Attendees of this session will come away with answers to hard questions: How do you prioritize incoming all-source cyber threat intel? What incidents meet your threshold of reporting and who do you call first? Finally, what resources and support can you expect in the event of a large-scale cyber incident affecting your organization?

Session IV: Under Attack: Foreign Adversaries and the Threat to National Security

In this session, FBI Special Agents working Counterintelligence matters will provide a briefing on state-sponsored tactics, techniques, and procedures to gain access and information in the private sector. It will also focus on how the private sector work with the U.S. intelligence community while concurrently protecting their information and infrastructure. The People's Republic of China (PRC) government remains a top adversary as it works to undermine U.S. rule of law, U.S. economic security, and fundamental human rights. Learn about how the FBI counters this threat, how you can recognize the threat, and how you can counter these adversarial operations while protecting your intellectual property.

Session V: Hunting The Enemy Within: Insights from a Mature Insider Threat Program

The proliferation of insider threats is a complex and persistent challenge for organizations across all sectors, charged with protecting their sensitive information and trade secrets from adversaries in today's threat-rich environment. The costs and consequences of an insider threat incident can be staggering, with particular implications to homeland security. Detecting, investigating and remediating insider threats requires navigating complex employment and privacy issues, a global understanding of regulatory and cultural issues, and limited avenues for remediation. This session will discuss how to develop a comprehensive cross-functional insider threat program that spans the incident lifecycle from prevention to mitigating the harm caused by a malicious insider.

Session VI: The Moment of Boom: Attacks on American Soil

Critical infrastructure is an attractive target for foreign adversaries because of the potential to disrupt our way of life. The interdependence and connectedness of our systems requires businesses to plan for the convergence of cyber and physical attacks. This session will feature case studies of attacks on American soil that leveraged cyber vulnerabilities and important lessons learned.

Session VII: The End Game: Putting Your Cyber Investigation on Trial

In this mock trial, learn how facts and evidence from a privileged cyber investigation are used as evidence during trial. Learn what the attorney-client privilege and work product doctrine protects (and doesn't protect) in litigation. Hear testimony from forensic experts, information security professionals, and arguments from both plaintiffs and defense counsel.

Session VIII: Harnessing Your Superpowers: The Business of Cyber

To win the cyber war, security leaders must proactively manage and address risks facing their organizations. The systemic risks rooted in supply chain threats, a changing regulatory landscape, and failure to understand the business context of current and future risks places an organization and its employees, customers, and stakeholders at risk. Learn how to conduct a cross-functional cyber risk assessment to tie cyber risk into a business context, improve decision-making and educate enterprise stakeholders from the board, executive leadership, management and workforce to better protect what really matters.

This session will also cover the importance of public/private partnership and programs like InfraGard® that are leading the way in securing U.S. critical infrastructure.