



# 2024 Let's Talk Security Agenda

## Fairmont Grand Del Mar

Great speakers. Beautiful location. Exceptional experience.

Wednesday, Nov 6<sup>th</sup> – Friday, Nov 8<sup>th</sup> 2024

5300 Grand Del Mar Ct, San Diego, CA 92130

**LET'S  
TALK**  
SECURITY

Wednesday, Nov 6<sup>th</sup>

4:30–5:30PM – Canyon Terrace

## Welcome Reception

5:30–7:30PM – Off-Site

## Private Dinner (Invite-Only)



Thursday, Nov 7<sup>th</sup>

9:00–12:00PM – Ballroom A-3

## Demo Day

Friday, Nov 8<sup>th</sup>

8:00–9:00AM – Northwest Foyer / North Foyer / North Courtyard

## Registration & Continental Breakfast

9:00–9:50AM – Ballroom A-1

## There is no Ozempic for Cybersecurity

Sponsored by **K logix**

There are no silver bullets or magic wands in cybersecurity. The most important trait in any CISO is persistence. Focusing on the basics, continuing to communicate and educate stakeholders, and always seeking to refine and improve security controls makes a security program successful. In this presentation, our panel of experts who have worked with every type of organization, from Fortune 10 to small mom-and-pop shops, share the key areas of focus that they wish every security program would pursue and share with the audience some of the ways you can overcome common challenges to get your security program looking the way you want it to look.

**Moderator:** Ryan Spelman, Managing Director, Cyber Risk at K logix

**Panelist:** Imran Jaswal, Founder at Swiftwater & Company

**Panelist:** Shay Colson, Managing Partner at Intentional Cybersecurity

**Panelist:** Sheela Kinhal, Vice President, Information Security GRC, Third Party Risk, & Model Risk at Green Dot Corporation

Continued 

9:00–9:50AM – [Ballroom A-2](#)

## AI in Cybersecurity

- Explain how AI and machine learning can enhance cybersecurity by automating threat detection and response.
- Share success stories of AI-driven cybersecurity solutions in action.
- Discuss the limitations and challenges of relying on AI for cybersecurity.
- Explore the need for human-AI collaboration in cybersecurity operations.
- Emphasize the ongoing research and development in AI for proactive defense strategies.
- Explain how AI and machine learning can enhance cybersecurity by automating threat detection and response.

**Moderator:** Kelli Tarala, Principal Consultant at Black Hills Information Security

**Panelist:** Vasu Nagendra, CEO, Founder at Alertwise

**Panelist:** Colin Theseira, Cybersecurity Project Manager at Boston Scientific

**Panelist:** Brian DeMuth, Partner / Co-founder / General Partner at Riphean Investments

**Panelist:** Patrick Simon, President and Manager at Beehive Technology Solutions LLC

9:00–9:50AM – [Ballroom A-3](#)

## AI-Powered Social Engineering

- Define AI-powered social engineering and its potential impact on individuals and organizations.

- Discuss how ChatGPT and similar AI models can be leveraged in social engineering attacks.
- Explore the psychological aspects of AI-driven manipulation and its effectiveness.
- Share case studies or examples of AI-based social engineering attempts.
- Propose countermeasures and user education to defend against AI-driven social engineering tactics.

**Moderator:** Alex Veytsman, CTO | Managing Partner | Chairman of the Board at Artificial By Design

**Panelist:** Darin Andersen, Chairman & CoFounder at NXT Robotics

**Panelist:** Omid Aloos, Solutions Engineer at Kitchen Armor

**Panelist:** Mark Willis, Freelance Privacy and Security Consultant

**Panelist:** Joe Erle, Insurance Specialist at C3 Risk & Insurance Services

**Panelist:** Ryan Freeman-Jones, Partner at Meditology Services

**Panelist:** Marc Kase, Managing Director at Achieve Agility, Inc.

9:50–10:05AM – [North Foyer / North Courtyard](#)

## 15-Minute Exhibit Hall Break

10:05–10:55AM – [Ballroom A-1](#)

## The Idea That You Can Protect, Sabotage or Just Misuse Your Companies, Infrastructure, and or Data Using Today's AI tools, and Generative Models will be Discussed

Sponsored by [Regents & Park, Inc](#)

Continued 

AI-driven cybersecurity tools, like Microsoft Copilot and CrowdStrike Falcon, enhance threat detection and response by automating processes and providing real-time forensics. However, cybercriminals use AI for more sophisticated attacks, such as phishing and deep fakes. To stay ahead, organizations must integrate AI into security strategies while managing risks like data breaches through strict governance and secure system configurations.

**Moderator:** Hessam Toudiee, Managing Partner at TodiTech

**Panelist:** Jason James, Partner & vCISO at Regents & Park, Inc

**Panelist:** Bryan Schader, Partner Risk Advisory & Compliance at Moss Adams

**Panelist:** Dr. Victor Monga, Global Cybersecurity Technologist at Menlo Security Inc.

10:05–10:55AM – **Ballroom A-2**

## Zero Trust – Another Security Buzzword or a Real Paradigm Shift?

Zero trust is gaining momentum as organizations increasingly reject outdated perimeter-based strategies. As organizations have begun to adopt a zero trust strategy, many best practices and lessons learned have emerged. At the same time, there are numerous misperceptions surrounding zero trust, especially with regard to legacy systems. This panel will provide concrete tips and different approaches to zero trust, while also addressing any perceived challenges that may be preventing organizations from pursuing a zero trust strategy.

**Moderator:** Robert Allende, Cyber Practice Lead at Red River

**Panelist:** Aaron Williams, Regional SLED Director CA & HI at Broadcom Software

**Panelist:** Andy Lin, Chief Information Security Officer at Brighton Health Plan Solutions

**Panelist:** Will McGuire, Director, Cybersecurity at XiFin, Inc.

**Panelist:** Rick Moy, Managing Partner at DeepLight Digital

10:05–10:55AM – **Ballroom A-3**

## ChatGPT and Data Privacy

- Highlight the importance of data privacy in AI-driven applications like ChatGPT.
- Discuss concerns regarding data collection, storage, and usage in conversational AI.
- Explore the role of encryption and secure data transmission in protecting user interactions.
- Examine the implications of data breaches or leaks involving AI-generated content.
- Offer best practices for organizations to uphold data privacy while using ChatGPT


**Moderator:** Sheela Kinhal, Vice President, Information Security GRC, Third Party Risk, & Model Risk at Green Dot Corporation

**Panelist:** Salma Debar, Privacy Risk Manager at Deloitte

**Panelist:** Kier Lane, Founder and CEO at ID-Y

**Panelist:** Brett Nakfoor, Sales at Red Access

**Panelist:** Ronald J. Hedges, Principal at Ronald J. Hedges LLC

Continued 

10:55–11:10AM – North Foyer / North Courtyard

## 15–Minute Exhibit Hall Break

11:10–12:00PM – Ballroom A-1

### Cybersecurity Insurance: The Good, the Bad, and The Risky

Sponsored by ICE Cybersecurity

This panel discussion will explore the evolving landscape of cybersecurity insurance, focusing on regulatory changes, premium trends, and the accuracy of risk assessments in an increasingly complex threat environment. Panelists will discuss the changing techniques in underwriting, post-incident response, and strategies for CFOs to ensure they're not overpaying for cyber coverage. The conversation will also highlight the importance of board-level awareness (Tone at the Top) and legal protection in managing cyber risks effectively.

- Moderator:** Ford Winslow, CEO at ICE Cybersecurity
- Panelist:** Erik Nakamura, Chief Financial Officer at Orange Comet, Inc.
- Panelist:** Phil Ducoffe, Senior Vice President, Risk Management at USI Insurance Services
- Panelist:** Matt Stamper, Chief Executive Officer at Executive Advisors Group, LLC
- Panelist:** Elaine Harwell, Partner at Procopio, Cory, Hargreaves & Savitch LLP
- Panelist:** John Driver, Chairman and CEO at Lynx Technology LLC

11:10–12:00PM – Ballroom A-2


## Cybersecurity Training

In 2024, will we see continued advances in cybersecurity training? Humans didn't evolve to spot dangers in the digital world. The school system doesn't teach them defense against the dark arts of cyber-attack. It's on us. Human risk is an organizational problem. Equipping our people with the skills to stay safe from phishing attacks is our responsibility.

Automation, adaptive learning, and artificial intelligence/machine learning can help deliver personalized training at scale. Why is that important? Because people need to participate frequently with relevant training that stays at the edge of their skill level in order to improve and stay engaged. A long, dry video followed by a punishment based phishing simulation has been proven not to work. Fixating on failure leads to failure.

Rewarding people as they acquire skills in a dynamic learning environment confers measurable improvement. This approach broadly describes gamification, whose demonstrated success is grounded in established principles of behavioral science and business and will be key to protecting organizations of all sizes in the year ahead.

- Moderator:** Terry McDaniel Jr., President, Retail at TPV Solutions Corp
- Panelist:** Alan Sugano, President at ADS Consulting Group, Inc.
- Panelist:** Brian Mendenhall, WW Head, Security & Identity Partnerships at Amazon Web Services (AWS)
- Panelist:** Ana Nicacio, Associate General Counsel at Epson America, Inc.
- Panelist:** E.J. Hilbert, Owner at KCECyber.com / KCEAdvisors
- Panelist:** Trisha Willbrand, Senior Cybersecurity Consultant at REDW

Continued 

11:10–12:00PM – [Ballroom A-3](#)

## There are not Enough Unicorns, Purple Squirrels, and Super Heroes to go Around

The talent shortage in cybersecurity goes much deeper than what we can solve with recruiting and education alone. In this panel discussion, we'll look at more productive ways to frame the problem we are facing and explore alternatives for finding the talent we need to succeed in our mission.

**Moderator:** Alexander Neff, Sr. Director of Information Security and Compliance at Faro Health Inc.

**Panelist:** Jen Greulich, Co-Founder/Chief Operating Officer at Legato Security

**Panelist:** Anthony La Scala, Director of Cybersecurity Operations at Infracore

**Panelist:** Cristian Ruvalcaba, Senior Cyber Security Technical Specialist at IBM

**Panelist:** Renee Small, Cybersecurity Super Recruiter at Cyber Human Capital

**Panelist:** Chaunce Hazelton, Founder & CEO at Vulnalysis

12:00–1:00PM – [North Foyer / North Courtyard](#)

## Lunch

1:00–1:50PM – [Ballroom A-1](#)

## Data Visibility, Compliance and Information Governance

Sponsored by [Ingenious Dataworks](#)

In 2024, CISOs will prioritize adopting solutions that provide visibility into the data their organization holds, where it lives, and the risks imposed by that data. This visibility is critical for security leaders as they build programs to meet compliance requirements in a highly regulated world, and secure data in an increasingly challenging threat landscape. One of the first laws in cybersecurity is that you need to know your assets. Simply put, you can't protect what you don't know. Join us, as we discuss the value of data classification and information governance.

**Moderator:** Chris LaCour, Co-Founder & CEO at Ingenious Dataworks

**Panelist:** John Martin, Co-Founder & CTO at Ingenious Dataworks

**Panelist:** Mansi Thakar, Staff Security Analyst at NVIDIA

**Panelist:** Jerome Prescod, Content Security Staff Engineer at The Walt Disney Studios

**Panelist:** Pergrin Pervez, Cybersecurity Lead at Stratascale – An SHI Company


**Panelist:** Glen Day, CEO at NVISIONx

**Panelist:** Jack P. Flaherty, Speaker / Author / Consultant / C-Suite Advisor at The Decision Switch™

1:00–1:50PM – [Ballroom A-2](#)

## Cyber Risk Management Will be a Top Priority for Business Leaders in 2024

When it comes to the governance and oversight of cyber risk, our system is broken. It's no longer what it used to be fifteen years ago – we are dealing with higher stakes and fragile enterprise reputations. As a result of this, in 2024, we will see companies double down on cyber risk management.

Continued 

Boards will need to have a much clearer role and responsibility when it comes to the process of ensuring adequate controls and reporting cyberattacks. Cyber risk governance is not just the domain of the CISO it is now clearly a Director and Officer level concern. When it comes to cyber, plausible deniability is dead. Join us, as we discuss best practices for cyber risk.

**Moderator:** Kamran Salour, Cybersecurity and Privacy Attorney at Lewis Brisbois

**Panelist:** Nishum Gupta, Chief Operating Officer at WhiteLint Global Pvt Ltd

**Panelist:** Craig Payne, Managing Partner at Payne Data Security

**Panelist:** Gregory Kemper, Senior Manager, Security Risk and Compliance at Sony Interactive Entertainment

**Panelist:** Rich Lindberg, Chief Information Security Officer at JAMS

**Panelist:** Allison Berres, Director of Global Sales at CyberSaint

**Panelist:** Greg Spicer, Co-Founder & Chief Revenue Officer at Ostrich Cyber-Risk

**Panelist:** Andrew Shea, Founder at CRFQ

1:00–1:50PM – [Ballroom A-3](#)

## Escalating Cyber Risk From the IT Department to the Boardroom

Despite today's frequent headlines regarding companies falling victim to cyberattacks or suffering data breaches, cyber risk is still a relatively new threat – is it? While companies may have an idea about the potential

effects on reputation and impact on the overall business, many are yet to experience one first-hand, or at least not on a high-profile scale. That means there's still unfamiliarity around how exactly to manage the risk. Many companies are changing their approach, in some cases; cybersecurity is still departmentalized and seen as the remit of the IT team.

- How do you incorporate a cybersecurity strategy into the company's overall governance, risk, and compliance structure? What's the best approach?

**Moderator:** Rhonda Jenkins, Founder & Senior Consultant at RJ Gets It Done

**Panelist:** Vidya Murthy, Chief Operating Officer at MedCrypt

**Panelist:** Shannon Brewster, Executive Director | General Manager | Security Consulting Services at AT&T

**Panelist:** Stanley Feinstein, President at Project Remedies Inc

**Panelist:** Areg Alimian, Partner at SmartGateVC

**Panelist:** Eric Herzog, Chief Marketing Officer at Infinidat


**Panelist:** Ray Li, Vice President of Product Development at Life Line Screening

**Panelist:** Javier Sotelo Felix, Principal Consultant at Asesco Consulting

**Panelist:** Ed Covert, Head of Security Risk Engineering at Bowhead Specialty

1:50–2:05PM – [North Foyer / North Courtyard](#)

## 15-Minute Exhibit Hall Break

Continued 

2:05–2:55PM – [Ballroom A-1](#)

## Malicious and Black Market Language Models (LLMs)

- Define what malicious use of LLMs entails, such as generating fake news, deep fakes, or phishing attempts.
- Discuss real-world examples of LLMs being exploited for illegal activities.
- Explore the challenges in detecting and mitigating malicious LLMs.
- Examine potential regulatory and ethical considerations for curbing black market LLMs.
- Suggest strategies for organizations and researchers to proactively counter this threat

**Moderator:** Kirk Hanson, Senior Sales Engineering Manager at Splunk

**Panelist:** Dimitry Dukhovny, vCISO, Security and Compliance Consultant at Security Standard LLC

**Panelist:** Dr. Ulrich Lang, Founder & CEO at ObjectSecurity

**Panelist:** Haydar Majeed, VP of Security | CTO at Privatyze

**Panelist:** Oksana Denesiuk, Sr. Product Manager | Solution Consultant – Billing at Kaiser Permanente

**Panelist:** Cho-Nan Tsai, President and CEO at Hyperionsoft

**Panelist:** Charles Renert, VCISO & Principal Advisor at ICE Cybersecurity

2:05–2:55PM – [Ballroom A-2](#)

## Building a Security-Aware Culture in 2024 and Beyond

Perhaps the most important step that can be taken at any organization is to ensure that it is working towards initiating and fostering a culture of awareness around cybersecurity issues. Today, it's no longer good enough for employers or employees to simply think of cybersecurity as an issue for the IT department to take care of. In fact, developing an awareness of the threats and taking basic precautions to ensure safety should be a fundamental part of everyone's job description in 2024!

Phishing attacks rely on "social engineering" methods to trick users into divulging valuable information or installing malware on their devices. No one needs technical skills to learn to become aware of these types of attacks and to take basic precautions to avoid falling victim. Likewise, basic security skills like the safe use of passwords and developing an understanding of two-factor authentication (2FA) should be taught across the board and continually updated. Taking basic precautions like this to foster a culture of cybersecurity-awareness should be a core element of business strategy at organizations that want to ensure they build resilience and preparedness over the coming 12 months.

**Moderator:** Patricia Gatley, Sr. Counsel and Compliance Officer at Prometheus Laboratories Inc.

**Panelist:** Austine Ohwobete, Cybersecurity Strategizing & Litigation at Cryptoforensics Technologies Corporation

**Panelist:** David Wayland, Senior Staff, Enterprise Security at BILL

**Panelist:** Janaki Desai, Independent Consultant

**Panelist:** Timothy Toohey, Partner Intellectual Property and Cyber-Security Practice at Greenberg Glusker LLP

**Panelist:** Justin Beals, CEO, Co-Founder at Strike Graph

**Panelist:** Kelly Worthington, Senior Business Consultant – Risk & Cyber Strategy at Tata Consultancy Services

Continued 



2:05–2:55PM – [Ballroom A-3](#)

## Data Breaches: Prime Target

Data will continue to be a leading concern for organizations around the world. Whether it be for an individual or organization, safeguarding digital data is the primary goal now. Any minor flaw or bug in your system browser or software is a potential vulnerability for hackers to access personal information. New strict measures General Data Protection Regulation (GDPR) was enforced from May 25th, 2018 onwards, offering data protection and privacy for individuals in the European Union (EU). Similarly, the California Consumer Privacy Act (CCPA) was applied after January 1st, 2020, for safeguarding consumer rights in the California area.

**Moderator:** Ronald J. Hedges, Principal at Ronald J. Hedges LLC

**Panelist:** Jerry Locke, Snowflake Practice Leader at Perficient

**Panelist:** Paul Caiazzo, Vice President at Quorum Cyber

**Panelist:** Katie Oliver, Paralegal at Scott+Scott

**Panelist:** Mike Anderson, Director Advisory Cybersecurity West Coast at Zyston LLC

**Panelist:** Brad Kelso, Managing Partner / Co-Founder at Privageo

2:55–3:10PM – [North Foyer / North Courtyard](#)

## 15-Minute Exhibit Hall Break

3:10–4:00PM – [Ballroom A-1](#)

## How to Address the Weakest Link in Cybersecurity – People

Cyber-crime statistics estimated the global cost of \$6 trillion in 2024. Cyber criminals continue to evolve their attacks faster than security professionals can adapt. But is the weakness with the technology in place to combat malicious actors or is it the people in the organization who continue to fall prey to the common tactics such as phishing? Every business owner, executive, and board member is now hypersensitive to the impact from cyber-crime but continue to focus on tools and technology.

Many organizations invest in cyber awareness programs to educate their employees and contractors and now are mandatory in many industries today but the number of breaches continues to increase. Therefore, the approach to improving the cybersecurity defenses must elevate to re-engineering the “DNA” of all resources – inside and out – to think cyber smart.

This panel will discuss ideas to help materially change the conversation about cyber awareness so anyone in contact with a business is cyber vigilant.

**Moderator:** Benjamin Brink, Vehicle and Mobility Cloud Security Engineer at TEKsystems

**Panelist:** Michael Martin, Cybersecurity Specialist at Technology & Services Industry Association (TSIA)

**Panelist:** Misha De Larkin, Sr. Director, IT Risk Management & Governance; Global ERG Business Partner at Flex

**Panelist:** Michael Giske, Interim/Fractional CTO/CIO at CTO/CIO Advisory Services

**Panelist:** J. Craig Williams, Founder at WLC | The Williams Law Corporation

**Panelist:** Dahlia Abrams, Sales Director at ClearTech

Continued 

3:10–4:00PM – **Ballroom A-2**

## Insider Threats

Human error is still one of the primary reasons for the data breach. Any bad day or intentional loophole can bring down a whole organization with millions of stolen data. Report by Verizon in data breach gives strategic insights on cybersecurity trends that 34 percent of total attacks were directly or indirectly made by the employees. So, make sure you create more awareness within premises to safeguard data in every way possible.

**Moderator:** Chris Loehr, EVP, CTO, CFC Response at CFC

**Panelist:** Matthew Hoy, Sr. Staff Cyber Technical Specialist – Incident Response at Albertsons Companies


**Panelist:** Sufyan Subzwari, Chief Information Officer and Executive Partner at DNAMIC

**Panelist:** Serge Jorgensen, Partner at Sylint

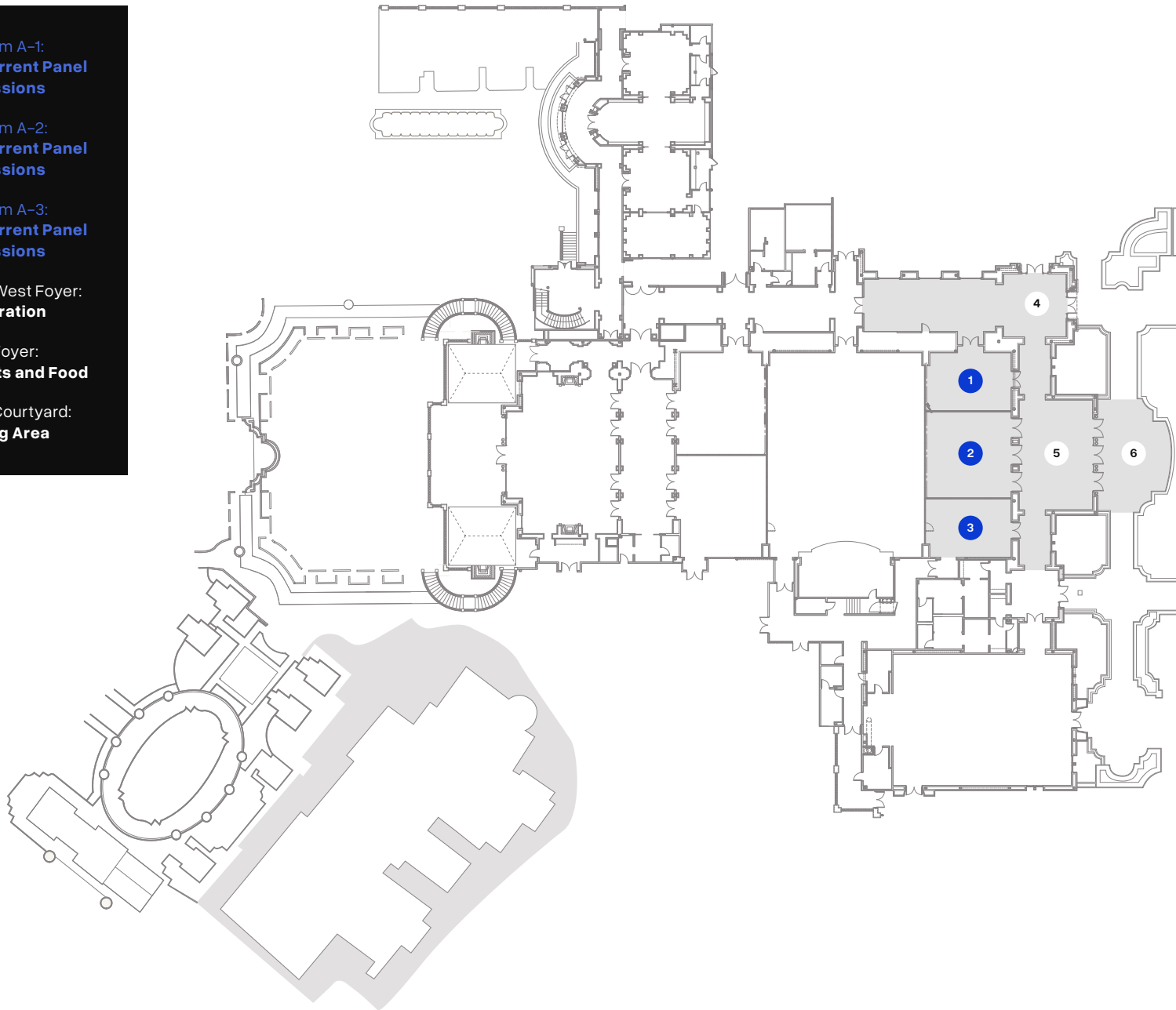
**Panelist:** Shelly Pruden, Staff Manager – Identity & Access Management at Qualcomm

**Panelist:** Jack McCready, CEO/CTO at JWM Consulting LLC



Continued 

1. Ballroom A-1:  
**Concurrent Panel Discussions**
2. Ballroom A-2:  
**Concurrent Panel Discussions**
3. Ballroom A-3:  
**Concurrent Panel Discussions**
4. North West Foyer:  
**Registration**
5. North Foyer:  
**Exhibits and Food**
6. North Courtyard:  
**Seating Area**



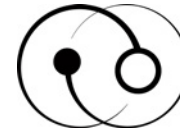
Continued 

# Sponsors

---



INFINIDAT



STRIKEREADY

CATO  
NETWORKS

 Strike Graph



  
legato security



INFYNITEONE  
TECHNOLOGIES

DRATA

 logix

NVISIONxx  
PROTECT THE JEWELS. PURGE THE JUNK.

IGD INGENIOUS  
DATAWORKS



**LET'S  
TALK  
SECURITY**

Contact

Events@LetsTalkSecurity.com



(949) 346-3846



LetsTalkSecurity.com



530 Technology Dr

Suite 100

Irvine, CA 92618

