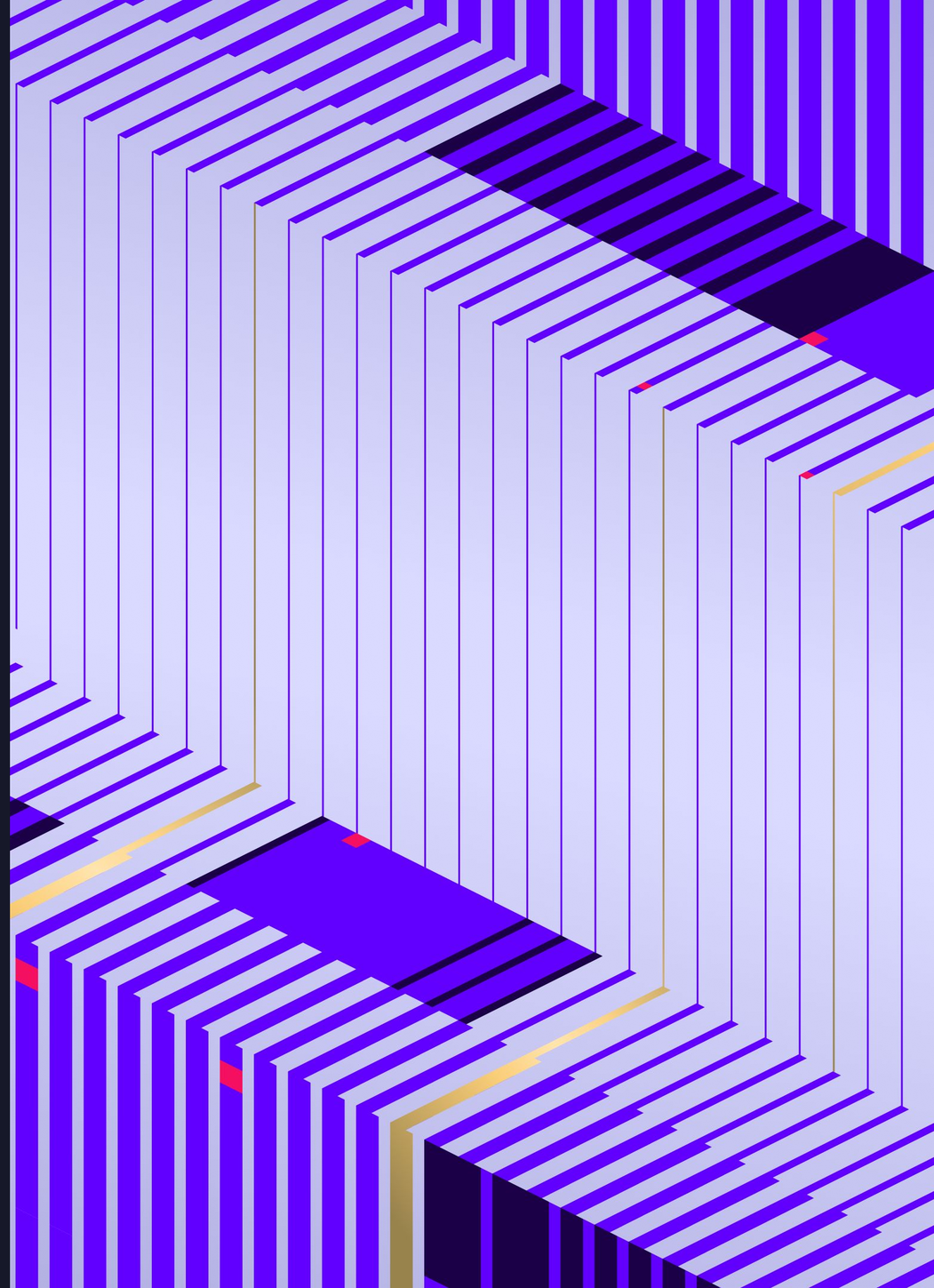
Charleston CyberLaw Forum

January 23, 2025

SentinelOne
Secure Tomorrow

CHARLESTON
SCHOOL OF LAW

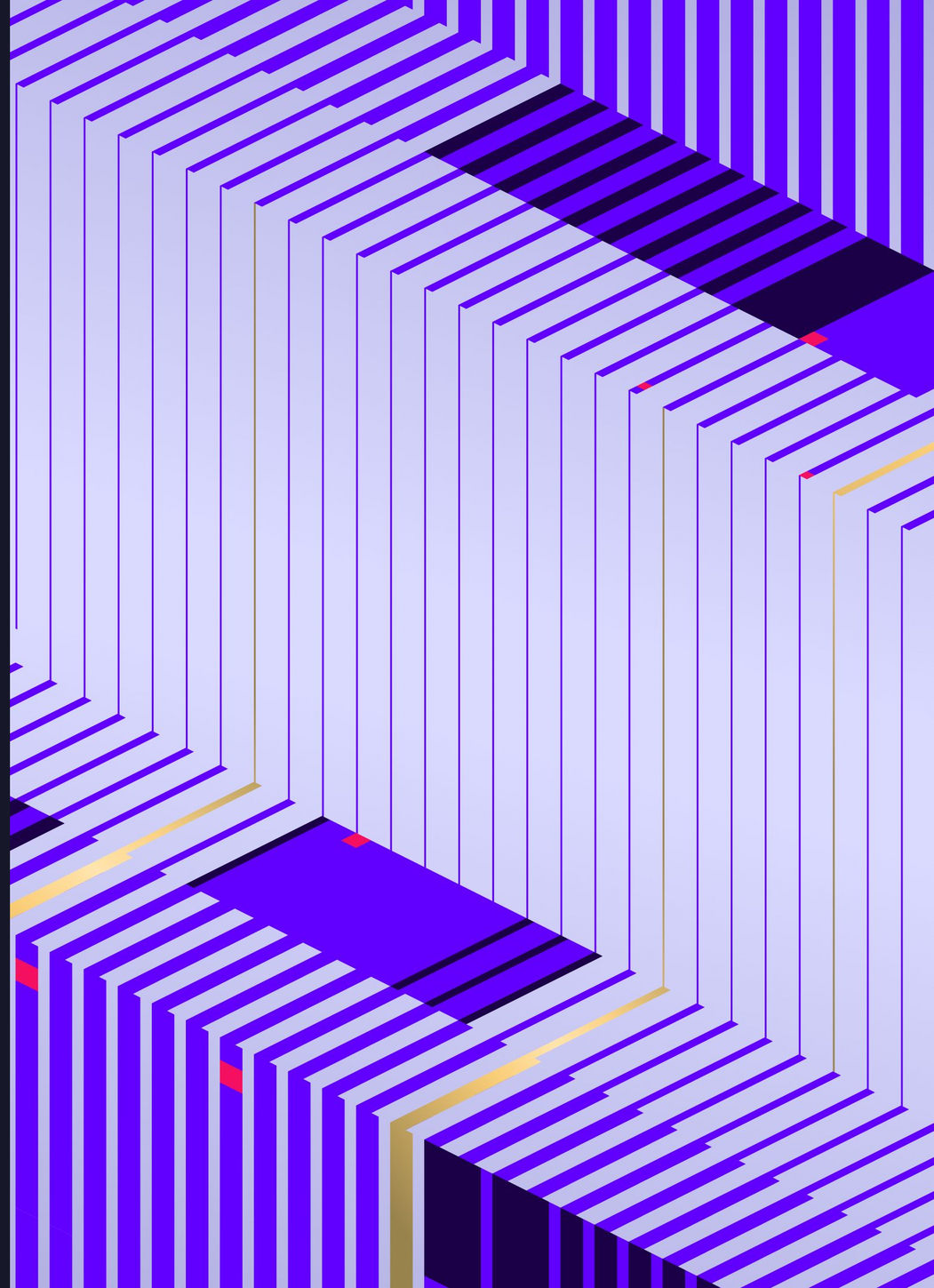


Keynote Fireside Chat

The CLE materials are sponsored by SentinelOne and Charleston Law School. All CLE materials are prepared by law firms and attorneys as noted in the materials, and do not offer any specific legal advice or guidance.

SentinelOne®
Secure Tomorrow

CHARLESTON
SCHOOL OF LAW



Presenters

Luke Dembosky

Co-Chair Global Data Strategy & Security

Debevoise & Plimpton

Brendan Rooney

VP Global Commercial IR

Booz Allen

Discussion

Cyber Risks to Critical Infrastructure and How Best to Prepare

SentinelOne

SentinelOne Secure Tomorrow

CHARLESTON SCHOOL OF LAW

Topics for Discussion

Vendor/Supply Chain Attacks Remain the Greatest Challenge

Resurgence of Insider Threats

Evolution in Extortion Schemes

Top-of-Mind Challenges for Companies

Luke Dembosky

Debevoise & Plimpton

Co-Chair Global Data Strategy & Security, Debevoise & Plimpton

Luke Dembosky co-chairs Debevoise & Plimpton's global Data Strategy and Security practice. He advises companies on managing cyber risks, responding to cyber incidents, and handling related internal investigations and regulatory defense.

Mr. Dembosky is ranked Band 1 by *Chambers* for Privacy and Data Security: Cybersecurity. He is also ranked Band 1 among a select group of seven U.S. crisis management lawyers, and the only cyber specialist named in the Crisis & Risk Management rankings. *The Legal 500 US* includes Mr. Dembosky among a select group of "Leading Lawyers" on data privacy and protection. He is a frequent speaker and panel member for business, legal practice and educational groups across the country.

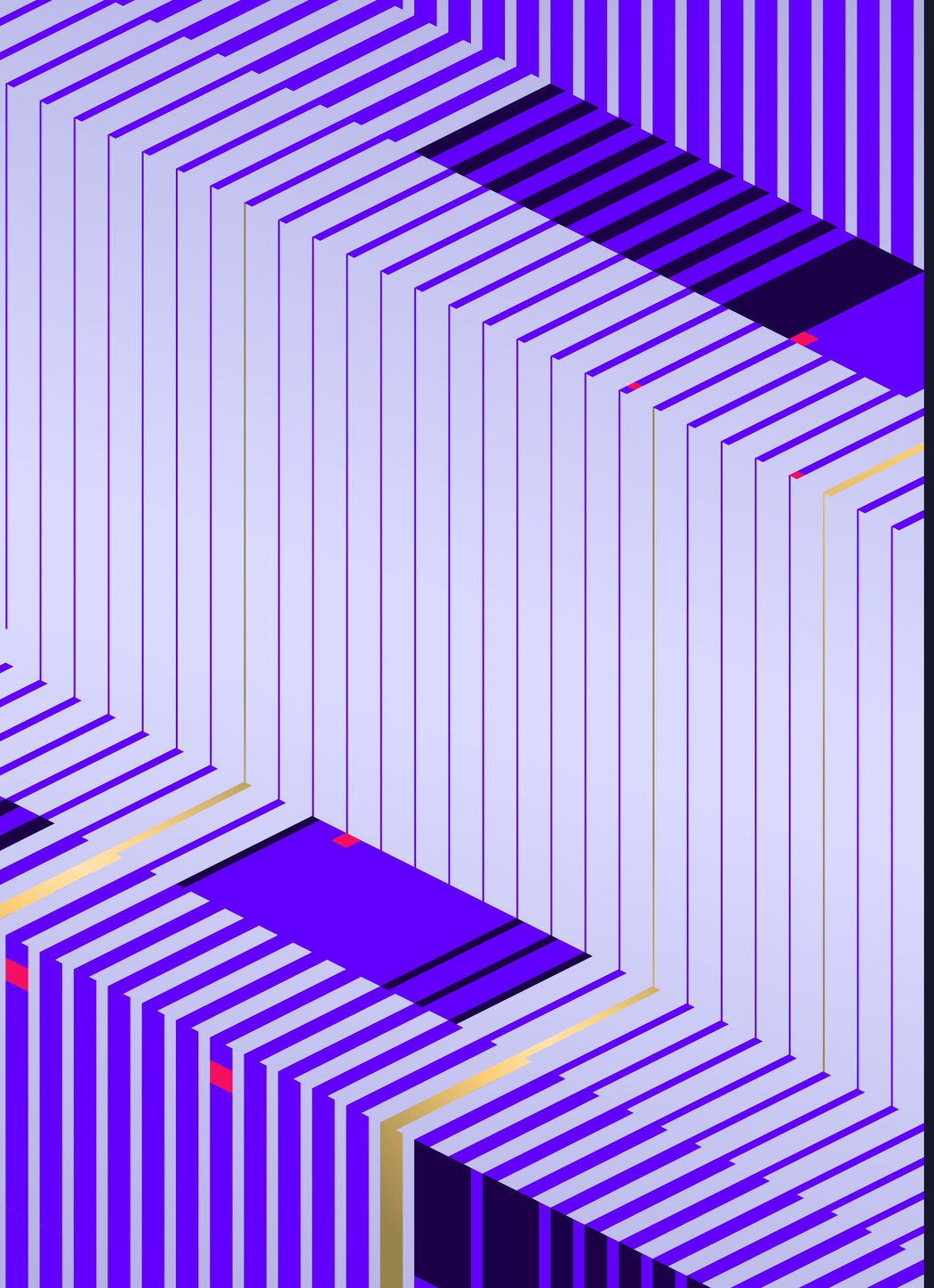
Mr. Dembosky joined Debevoise in March 2016 after serving as Deputy Assistant Attorney General for National Security at the U.S. Department of Justice, where he oversaw all national security cyber matters for the agency. His 14 years at DOJ included serving as DOJ's representative at the U.S. Embassy in Moscow, and as the senior DOJ official on the Target, Sony Pictures, Anthem, and OPM breaches, among many others. He has co-represented DOJ in cyber negotiations with Russia and China and at the UN Group of Government Experts.

Brendan Rooney

VP Global Commercial IR, Booz Allen

Brendan brings a diverse background in cyber risk, drawing upon prior roles in the cyber insurance and cybersecurity consulting industries. Incorporating business development, project management and threat intelligence, he works with companies around the world to identify, contain and eradicate threats from their digital environments. Brendan has worked with law firms, insurance carriers and directly with victims of complex cybersecurity compromises, maintaining active certifications as a CSI Linux certified investigator and open-source intelligence (OSINT) analyst.

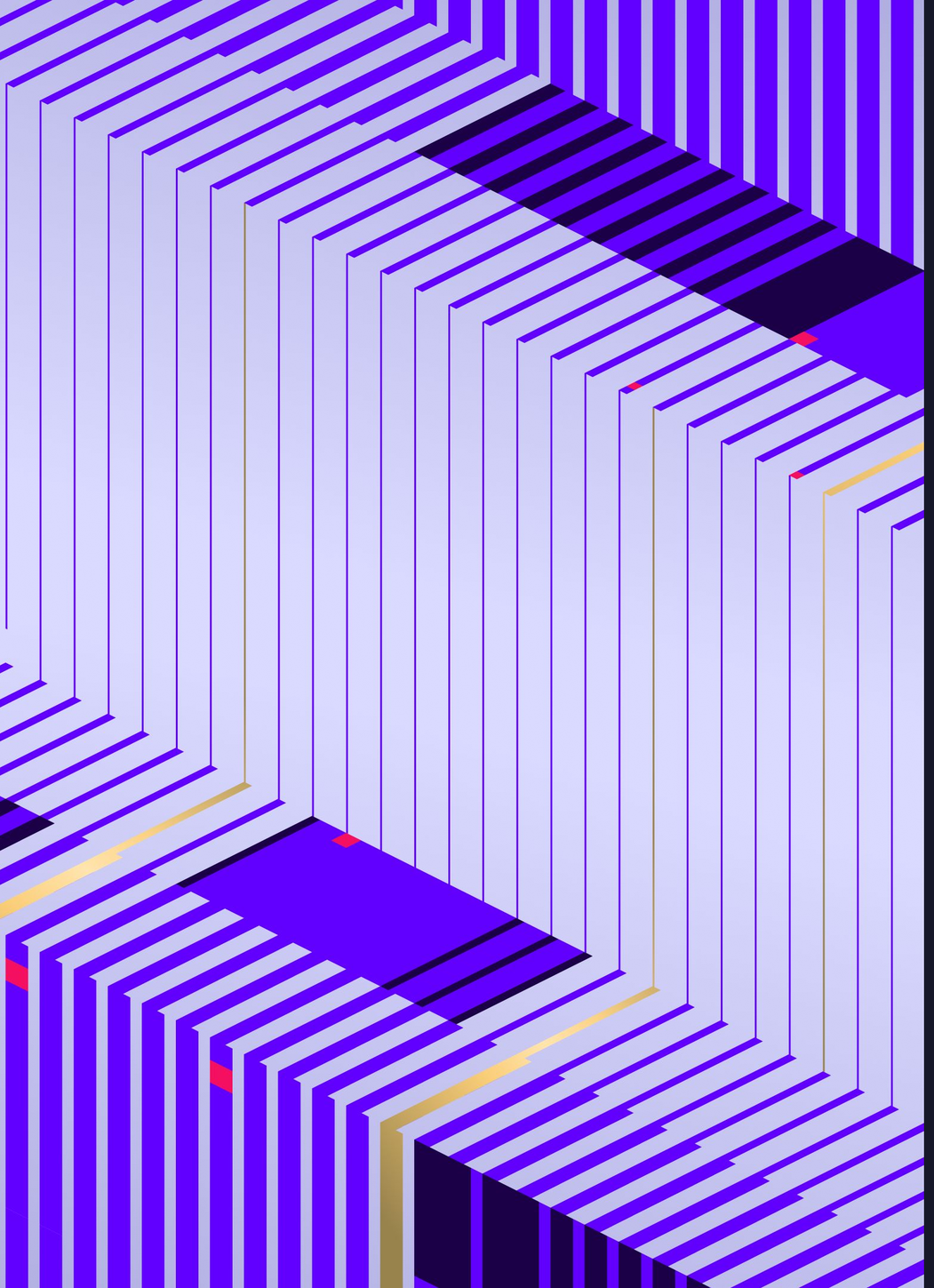
A frequent speaker on the topics of digital forensics and incident response, Brendan has led discussions on the prevention and response to cyber security incidents throughout the insurance, manufacturing, healthcare, financial services, education and public entity verticals.



SentinelOne
Secure Tomorrow

Thank You

Sentinelone.com



SentinelOne
Secure Tomorrow

Appendix

Sentinelone.com

Critical Infrastructure Issues

- Vendor/Supply Chain Attacks Remain the Greatest Challenge
  - Campaigns against telecoms and others
  - Geopolitical complexities add to the risk picture
- Resurgence of Insider Threats
  - Prolific remote IT workers scheme
  - Rogue job outsourcing and other means of behaving badly
- Evolution in Extortion Schemes
  - Changes in the ransom ecosystem
  - Fragmentation of leading groups
- Top-of-Mind Challenges for Companies
  - Right-sizing cyber engagement for senior leadership and board
  - Finding a strategy to address third and fourth party risks
  - Adapting traditional BCP/DR to cyber realities
  - Managing AI risks, including ones few are talking about

Critical Infrastructure - Context

1. Higher stakes with systemic supply chain attacks. The recent, widespread compromise of at least 9 major US telecoms is part of a troubling pattern of campaigns targeting critical infrastructure. Interception of sensitive communications is bad enough, but movement into OT systems for energy, water and food supply is another level of nightmare.

2. Insider threats via supply chain. The FBI says that just about every company that outsources remote IT has North Koreans in their employment. This has evolved from an edge threat to one of the most pervasive problems for major companies, and now includes data theft and elements of extortion in some cases.

3. Evolution in the extortion game. The ransom ecosystem has evolved tremendously since the time of monolithic threats like Maze and Ryuk. Today's ecosystem includes a wide range of supporting brokers, hosters, checkers, and others, along with ongoing fragmentation of alliances on top of RaaS trends that began a few years ago. Data extortion is now the fastest area of growth, and is increasingly combined with new leverage tactics that force organizations to change the way they prepare and respond.

Critical Infrastructure - Long Running Themes

The good news is that most regulators are gelling around a common set of cybersecurity concepts, albeit still with varying requirements. A strong foundational program will satisfy the vast majority, however:

- --We don’t know what will happen with CIRCIA or even CISA itself, but the choices made around extensive early reporting are likely (in my view) to cause more harm than good.
- --A large percentage of ransom attacks we encounter are launched to coincide with an important transaction, like an M&A closing, and therefore should change our OpSec around those key events.
- --BCP and DR are being tested broadly and generally have failed in the cyber context. What type of resilience and recovery challenges are unique to cyber and how do we change BCP and DR planning to account for them?
- --AI presents myriad new opportunities and risks. Sometimes the biggest risks are not the ones getting the most airtime at conferences or in board meetings.