Cybersecurity / AI Executive Roundtable Delves into Companies' Challenges in Addressing Evolving Cyber Threats

CHICAGO, May 14, 2026 – An Executive Roundtable exploring the challenges companies are facing on evolving cybersecurity threats, ransomware and AI concluded that those firms most vulnerable include those that fail to recognize cybersecurity as a governance and potentially existential issue. Experts also warned that when a cybersecurity event occurs, the average recovery time is 21 days, while the average amount of operating capital most middle-market firms maintain covers only 26 days.

Held in Chicago in April, the *Beyond the SOC* (Security Operations Center) roundtable featured a frank, in-depth discussion among a cross-disciplinary group of senior cybersecurity practitioners, financial services executives, legal counsel, insurance professionals and technology leaders – including officials who have managed some of the most high-profile cybersecurity breaches in the world. The event was organized and co-hosted by Mayer Brown, an international law firm with specialties including in AI and cybersecurity; Tölt Strategies, an independent compliance and regulatory advisory firm; Blue Team Alpha, a rapid response cybersecurity firm; and DIACSUS, a financial services advisory firm specializing in data, digital, risk, regulation, AI frameworks, transformation, merger and acquisition (M&A) due diligence and growth strategies.

The agenda focused on four core themes:

- **Managing Cybersecurity in an Evolving Threat Environment:** Bridging the gap between technical risk and financial impact.
- **'Punch Back':** Navigating the legal, technical and ethical friction of offensive cyber defense.
- **'True Recovery':** What genuine operational resilience looks like beyond backup tapes.
- **AI as a 'Force Multiplier':** Material changes to economics and effectiveness on both the attack and defense sides of the equation.

Roundtable participants flagged a structural misalignment between chief information security officers (CISOs) and financial leadership. Most organizations frame cyber risk in qualitative terms, not the dollar-denominated language that drives capital decisions for chief financial officers (CFOs), CEOs and Boards. An estimated 80% of organizations cannot put a dollar value on their own data or calculate the profit impact of an outage. The fix, participants concluded: CISOs must translate technical risk into financial terms – dollars lost per day from interruption or corruption – so leadership can resource and hedge against it appropriately.

Brad Giemza, moderator of the event and Advisor and Consultant to Tölt Strategies, said: "Cyber risk is still too often communicated in technical terms, while capital is allocated in financial ones. The organizations that will get this right are those that can translate security signals into clear economic impact in dollars at risk, downtime cost and business disruption so leadership can make informed decisions."

Ed Driscoll, CEO of Blue Team Alpha and a former U.S. Navy defense contractor, said that while AI threat triage is here, most company defenses still rely on manual triage, human escalation and analyst review, which he said are already obsolete. "Cybersecurity is no longer about humans attacking humans. It's now about AI-generated, autonomous attacks, and it's moving at speeds that no human team can match. AI detection is here, but we need to recognize that these threats are not just autonomous but bespoke as well. We're no longer living in a world where there is a known set of threat vectors to defend against. Bespoke AI attacks demand bespoke countermeasures deployed at machine speed with a 'human in the loop.'"

Participants also distinguished between compliance and security, noting that a firm that passed a System and Organization Controls (SOC) 2® audit may have met a baseline of compliance, but breaches don't happen at the baseline. Kirke Cushing, Partner of DIACSUS, said: "Ticking a box is transactional at best and not strategic. Breaches happen in the 0.1% gap that auditors or SOC controls don't test or assess well enough; think residual access, misconfigured permissions, and edge-case workflows and exceptions that became permanent by default. Attackers and adversaries are looking for this control gap, where no one internally is on top of it. Outside of identity controls, this is the next critical assessment space."

A number of participants wanted to discuss the latest thinking on "punching back," or going after attackers directly in cyber. Veronica Glick, Partner of Mayer Brown, said: "Attackers in today's world have low costs and a high upside, while defenders face high costs and constant pressure as they work to protect their companies against any potential threats. Within existing legal constraints, we are seeing growing interest in policy debates around active defense."

The U.S. Computer Fraud and Abuse Act (CFAA) enacted in 1986 broadly prohibits unauthorized access, encompassing virtually any offensive action against an attacker's infrastructure. Participants discussed that many elements of the Act may be outdated, creating risk but also potential opportunity around cyber policy. Despite the need for policy examination, an offensive approach could lead to risks, including inadvertently impacting the infrastructure of third parties, such as company consultants that may have been compromised. There is also the significant risk of triggering escalation or interfering with an active government intelligence operation, among others. Changes in policy would require a close look at these and other potential issues, participants said.

Driscoll said: “The CFAA is outdated, and the current environment creates both risk and potential opportunity around cyber policy. Firms with a material stake in critical infrastructure should engage in advocacy, rather than wait to react to legislative outcomes.”

Properly insuring against cyber risk – particularly when there could be a multi-billion dollar impact – is another major challenge. One participant pointed out that firms with annual revenues between $200 million and $1 billion are systematically under-insured. Boards routinely reject higher coverage tiers because the premium is deemed excessive, without rigorous analysis of the actual cost that a 21-day data and system shutdown would bring.

Dorothy DeWitt, founder and CEO of Tölt Strategies and former Director of the Division of Market Oversight at the U.S. Commodity Futures Trading Commission (CFTC), said companies may begin to “think outside the box” and utilize the power of curated prediction markets to guide major decision-making. She said companies can requisition a prediction market for cyber risk and recognize an outage risk as a priced probability, with continuous market-based signals driving the contract trading, helping companies decide how to allocate resources across prevention and insurance. “Such a vehicle could surface real-time probabilities and challenge internal corporate assumptions. Markets are extraordinarily efficient at pricing uncertainty, and cyber risk is the ultimate uncertainty.”

Participants also emphasized strongly that avoiding use of AI is not the way to defend against cyber risk. Rather, companies that fail to explore its potential risk losing out to competitors. “We see companies moving in the direction of autonomous detection, autonomous response and systems that can fight without waiting for approval,” Cushing said.

About Mayer Brown

Mayer Brown is a leading international law firm positioned to represent the world’s major corporations, funds, and financial institutions in their most important and complex transactions and disputes.

About Tölt Strategies

Independent regulatory and advisory firm Tolt Strategies, founded by Dorothy DeWitt, has a team of independent experts who tailor solutions to clients. The firm utilizes bespoke principal-level team structures, tailoring time-tested regulatory solutions to innovative industries and bringing recent senior government experience combined with decades of private sector pragmatism.

About Blue Team Alpha

Blue Team Alpha is a veteran-owned, comprehensive cybersecurity force on a mission to secure and defend America’s critical infrastructure. The firm offers advisory, offensive and technical services with deep roots and a specialty in incident management. The Blue Alpha Team has decades of experience handling breach investigations across all 16 critical infrastructure sectors, Over 65% of the firm’s experts are former nation-state-level employees from the Department of Defense, Department of Homeland Security and other government organizations.

About DIACSUS

DIACSUS is a global advisory and consulting firm to the financial services community, specializing in data strategy, data management, strategic AI-augmented operations, cyber security, risk management, regulation, transformation and integration capabilities. The firm also delivers buy-side commercial due diligence reviews for private equity firms. Led by partners Thomas Dunlap and Kirke Cushing, DIACSUS bridges the gap between technical risk and C-suite financial realities, guiding clients through complex compliance mandates, and core operating architecture.

Media Contact:
Ellen G. Resnick
Crystal Clear Communications
+1 312-399-9295 (mobile)
eresnick@crystalclearPR.com