TECHNOLOGY, MEDIA & TELECOM

Cybersecurity: Insights from Spring 2024's Premier Conferences

Lincoln International attended several of the foremost cybersecurity conferences globally in recent months. These gatherings are crucial as they bring together experts, executives, government officials and thought leaders to evaluate the global cyber landscape, gauge market trends and shape both public and private sector policies.

Below we share key insights from these conferences and what they mean for the cyber industry.

Cybertech Global (April 8-10, Tel Aviv)

Held annually in Tel Aviv, Cybertech Global brought together top executives, government officials and leading decision-makers across all areas of cyber. The event was attended by 20,000 participants, including multinational corporations, startups, private and corporate investors and venture capital firms.

While in Tel Aviv, the Lincoln team hosted a "Cybertech Soiree" where thought leaders across various cyber sub-verticals united to share their thoughts on the market landscape and strategize how to best position their teams and projects to align with shifting cyber trends and customer needs.

(continued on next page)

Despite Rising Geopolitical Tension, Israeli Cyber Industry Continues to Flourish

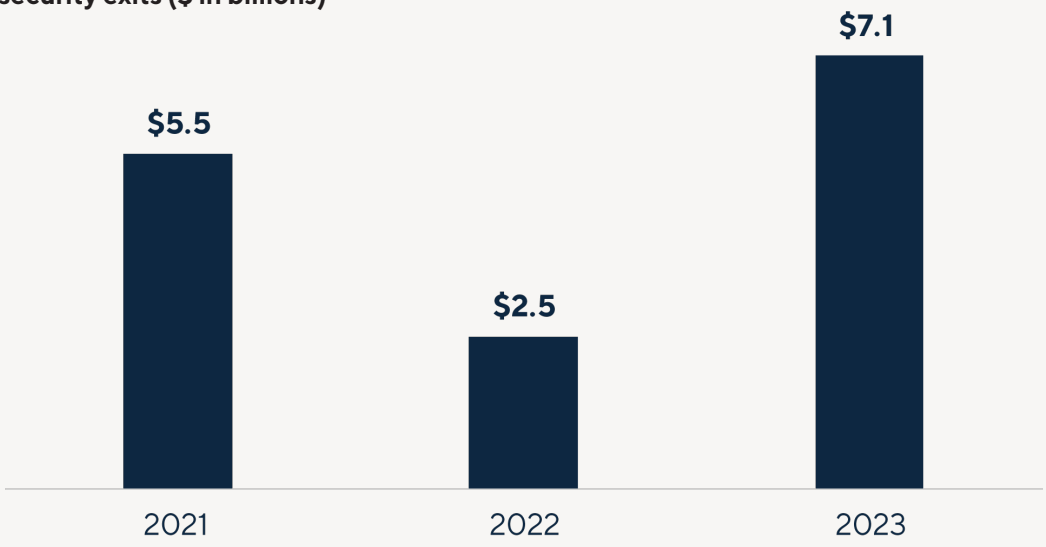
Amidst geopolitical unrest, Israel stands out for its cutting-edge technological achievements and engineering prowess, captivating attention and investments from around the globe. The Cybertech conference this year was a testament to this, pulling in cyber leaders from more than 60 nations.

While other sectors might falter under geopolitical strain, cyber sees a surge in interest and investment, and nowhere in the world has this been more impactful than in Israel. The country's cyber sector has flourished, benefiting immensely from years of government investments, fruitful collaborations between the public and private sectors and integration with the Israel Defense Force's specialized cyber units.

Additionally, the country stands as an epicenter for cyber transactions, experiencing an uptick in cyber mergers and acquisitions (M&A) and capturing 10% of the global cyber growth investment deal volume in 2023, according to Pitchbook.

Furthermore, 2023 saw the Israeli cyber industry achieve a remarkable $7.1 billion in exits, the sale of companies' ownership or stock, accounting for almost half of all tech sector exit transactions. Amidst a challenging geopolitical environment, the resilience of Israel's cyber industry shines through. Industry leaders and the sector at large press on with unwavering determination, which will allow the industry to emerge from the current crisis stronger than ever.

Israeli Cybersecurity exits ($ in billions)



Source: Cybertech Global and IVC report

(continued on next page)

Notable Israeli Cybersecurity M&A Exits in 2023 & 2024

Announced	Acquirer	Target	Deal Value
Jun-24	tenable	eureka	ND
Apr-24	WIZ	Gem	$350 million
Jan-24	zscaler	Avalor	$350 million
Jan-24	CROWDSTRIKE	FLOW.	$54 million
Nov-23	paloalto NETWORKS	TALON	$460 million
Sep-23	tenable	ermetic	$265 million
Sep-23	CHECK POINT	perimeter 81	$480 million
May-23	rubrik	Laminar	$225 million
Mar-23	CISCO	Lightspin	$160 million

Source: 451Research Screen

GISEC Global (April 23-25, Dubai)

Held annually in Dubai, the Gulf Information Security Expo and Conference (GISEC) is the largest cyber event in the Middle East. The event saw more than 750 of the top global cyber enterprises present to over 20,000 CISOs, government dignitaries and thought leaders from major corporations in over 130 countries across the Middle East, Africa and Asia.

The conference was highlighted by a Lincoln-hosted event curating a series of presentations on the region's market landscape. Speakers included two leading Gulf region cyber venture capital investors, a Gulf region security agency official and the Chief Executive Officer of a leading artificial intelligence (AI)-powered cyber platform, while Lincoln provided an overview of the growing demand for cyber in the Middle East and Africa.

(continued on next page)

Rising Cyber-Attacks Have Fueled Rapid Cyber Investment in the Middle East

GISEC's founding inspiration and a recurring theme of the conference highlighted the Middle East's increasing investment in cyber, spurred by the escalating frequency and financial implications of cyber-attacks in recent years. Kaspersky's research unveils that in the past two years, a staggering 87% of companies in the UAE have experienced a cyber incident. This uptick in cyber incidents has galvanized companies across the Middle East to ramp up their defenses against digital threats.

Reflecting this urgency, the Gulf Cooperation Council anticipates a significant expansion in the region's cyber market, projecting growth from the current $4.5 billion to an impressive $13.4 billion by 2030, according to Frost & Sullivan. This projection highlights not only the rising threat landscape but also the region's proactive stance in fortifying its digital frontiers.

The increasing need for cyber in the Middle East was a common topic of discussion as companies and investors seek to better understand how the rising threat of cyber-attacks will impact future business in the region. Discussions with attendees revealed a consensus on the pivotal role of AI as a shield against cyber threats and bad actors. Forecasts support that Middle East and North African AI spending will increase by a 44.8% CAGR from 2024 to 2030, expanding the total spend from roughly $12 billion today to almost $160 billion by 2030.

Safeguarding Critical Infrastructure is a Top Priority

GISEC sparked meaningful discussions among industry experts and governmental bodies, with a sharp focus on the importance of cyber for critical infrastructure. Reflecting the global pulse, the Allianz Risk Barometer positioned cyber-attacks on critical infrastructure as the second top cyber concern worldwide, signaling a broad consensus on the issue's criticality. The importance of the topic was discussed by multiple presenters. Dutch Railways Cyber Director and CISO Dimitri van Zantvliet highlighted how critical infrastructures relying on legacy systems, like transportation, are especially vulnerable to current cyber threats. With increasing connectivity across systems, breaches in one system may also lead to breaches across all interconnected systems, furthering the need for internet of things (IoT) cyber solutions.

Outside of transportation, energy was discussed as another especially vulnerable sector, with the emerging integration of operational technology (OT) and information technology (IT) systems as a concern. Mihir Joshi, the Chief Cyber and Information Officer at Tata Power, shed light on the challenge of implementing a unified security strategy for OT amidst expanding attack surfaces. As OT systems are integrated with IT for operational efficiency, the two systems having different vulnerabilities increases breach potential.

The discussions emphasized a critical call to action: the necessity for seamless collaboration between governments and the private sector. Together, they must forge regulatory alignments and promote open information exchange, reinforcing the bedrock of a globally robust cyber framework for critical infrastructure.

Public-Private Partnerships Emerge as a Crucial Strategy in Combatting Rising Data Breaches

Another key theme was the crucial role of public-private partnerships in addressing the rising tide of cyber threats and data breaches. GISEC brought together a diverse group of experts across various sectors to discuss and advocate for stronger collaborative efforts between governmental bodies and private organizations to bolster global cyber resilience. This year's emphasis was notably on sectors targeted within the Middle East, including oil, gas, government services and finance, reflecting worldwide concern over the breaches of more than 30 billion records in 2024.

(continued on next page)

The event showcased the significant, escalating financial impact of cyber breaches, with the average incident in 2023 costing around $4.5 million. These discussions underscored the urgent need for tighter cooperation across sectors to mitigate challenges. Experts like Saiful Islam from Dhaka Bank and Charles Brooks from Georgetown University emphasized the shift needed from merely reactive measures to the development of robust, proactive cyber contingencies. The emphasis was on the importance of leveraging joint resources, knowledge and strategies to better anticipate and neutralize threats.

The overwhelming consensus among attendees was on the necessity of forging and strengthening public-private partnerships to respond to and stay ahead of cyber threats. Through shared intelligence, advanced technologies and collective strategies, the conference solidified the belief in a unified approach to secure a more resilient digital infrastructure against the backdrop of ever-evolving cyber challenges.

Growing Importance of Dubai's Cyber Index

With an increasing emphasis on the importance of the UAE's strategic role in global cyber, the Dubai Cyber Index was highlighted as a key initiative. Launched in 2020 by H.H. Sheikh Hamdan bin Mohammad bin Rashid Al Maktoum, Crown Prince of Dubai, it proactively provides a comprehensive framework for businesses across the Dubai region to enhance cyber.

The index's objective is to address the complexity of security challenges in today's interconnected world and provides a playbook for bolstering defenses against emerging threats in the region by utilizing advanced technologies like AI for threat detection, response and recovery. Based on a recent Cisco study, 91% of UAE firms are integrating AI into their cyber strategies, underscoring the importance of the Dubai Cyber Index in guiding local businesses toward effective cyber resilience.

The Dubai Cyber Index was continuously touted as especially relevant in today's hyper-connected world, where increasingly complex security frameworks and sophisticated threats require more built-out, adaptable solutions.

RSA Conference (May 6-9, San Francisco)

Held annually in San Francisco, California, the RSA Conference is a leading cyber forum and exposition, bringing together industry experts, entrepreneurs, executives, investors, financial institutions and media. The conference had more than 41,000 participants from 130 countries, with 650 speakers and 600 exhibitors presenting to attendees and over 400 media members.

In tandem with the conference, Lincoln hosted its annual Cyber CEO Dinner. The event provided an opportunity for participants to connect with fellow chief executive officers from private cyber businesses, discuss strategic sector moves and learn about the dealmaking environment.

> **91%** of UAE firms are integrating AI into their cyber strategies

(continued on next page)

Vendors Continue to Focus on Profitability

Savings, rather than spending, emerged as a key theme this year. Cyber professionals are looking to do more with less, as balanced growth and profitability continue to be critical drivers for valuations.

Consider Palo Alto Networks, one of the foremost cybersecurity vendors. This year, the company made a statement by opting not to participate in the RSA Conference. Instead, the company hosted a private event at a separate venue, likely resulting in substantial savings to its sales and marketing budget. Palo Alto Networks only achieved profitability in 2022 and has since seen its sales and marketing expenses as a percentage of revenue drop significantly over the last several years.

In 2024, 95% of publicly traded cyber vendors expect to achieve a positive EBITDA margin, a notable increase from 52% in 2022, highlighting a strategic shift towards financial prudence and sustainable growth.

Cybersecurity Public Vendors EBITDA Margin

	2022A EBITDA Margin	2024E EBITDA Margin	2022A - 2024E EBITDA Margin Change
A10 Networks	21.6%	27.6%	6.1%
Akamai Technologies	31.7%	41.8%	10.1%
Check Point Software Technologies	39.0%	44.8%	5.8%
Cloudflare	(11.8%)	18.2%	30.0%
CrowdStrike Holdings	(5.3%)	25.9%	31.2%
CyberArk Software	(23.3%)	12.1%	35.5%
F5	19.8%	37.4%	17.6%
Fortinet	24.2%	29.7%	5.5%
Okta	(36.0%)	19.3%	55.3%
OneSpan	(3.1%)	21.9%	25.0%
Palo Alto Networks	0.6%	30.0%	29.4%
Qualys	33.7%	42.1%	8.4%
Radware	1.3%	10.0%	8.7%
Rapid7	(10.3%)	21.4%	31.7%
SecureWorks	(20.7%)	3.5%	24.2%
SentinelOne	(88.5%)	(1.6%)	86.9%
Tenable Holdings	(6.3%)	19.6%	25.8%
Trend Micro	25.3%	25.6%	0.3%
Varonis Systems	(23.0%)	4.5%	27.5%
VeriSign	69.5%	72.2%	2.7%
Zscaler	(26.6%)	21.7%	48.3%

Source: CapIQ (As of 5/31/2024)

Increasing Cyber Regulatory Activity is Driving Proactive Compliance

RSA 2024 also highlighted shifting mindsets towards the growing necessity for internal security protections and a deeper understanding of AI's roles in cyber. 68 tech companies including Amazon, Google, Cisco, Microsoft and IBM signed the U.S. Cybersecurity and Infrastructure Agency's "Secure by Design" pledge, committing to seven security goals over the next year. The objective is to provide a non-regulatory solution where signees report publicly how they progressed on each of the goals:

- Increased multi-factor authentication
- Default password reduction
- Reduction of system vulnerabilities
- Increased cadence of security patches
- Publishing of a vulnerability disclosure policy
- Increased transparency around common vulnerabilities and exposures
- Increased transparency to customers of intrusions affecting a company's product

This comes on the heels of increased regulatory pressures in both the U.S. and Europe, with the SEC taking new steps in regulation in 2023 and NIS2 expanding cyber mandates. As a result, the regulatory landscape around cyber, privacy and AI is driving the need for companies assisting with governance, while CISOs zero in on AI governance amid changing regulations.

Overall, RSA highlighted how increasing regulations are driving acquisitions and alliances to leverage AI for enhanced data protection and cyber solutions. As companies are looking for data-centric solutions in security to stay ahead of industry regulations, the conference signaled the trend toward consolidation in the cyber industry will continue.

Spotlight on AI Responsibility

A hot topic revolved around the influence of AI on the cyber landscape. The dialogue around generative AI has been a tightrope walk between its promising benefits and the apprehensions about its potential misuse in cybercrime. Industry practitioners are threading this line, wary of AI's capabilities in the wrong hands while optimistic about its power to enhance threat detection and response efforts.

A pivotal moment came with IBM's unveiling of its "Securing Generative AI" report during the conference, casting a spotlight on a concerning trend: AI development is not receiving the appropriate security. The report disclosed that only 24% of generative AI projects are secured, and an alarming 70% of survey participants believe innovation is being prioritized over security measures.

Despite the widespread enthusiasm and recognized potential of generative AI in various business spheres, the security of these initiatives seems to take a backseat for many executives in today's fast-paced environment. This situation highlights the critical need for a proactive, collaborative effort between cyber professionals and business leaders. Such a partnership is essential to lay the groundwork for the ethical, safe and secure employment of generative AI—a breakthrough technology that will reshape cyber and how businesses operate.

If you are interested in learning more about what we are seeing in the market, connect with a Lincoln cyber professional below.

For other perspectives, visit us at www.lincolninternational.com/perspectives.

Get to know Lincoln's Technology, Media & Telecom Group.