Q2 2023 Cyber Security Update

Cyber Security News/Insight

- During the period 2016-2022, the cybersecurity market grew at an annual rate of 12.1%, to a market size of $147.4 billion in 2022.[1] Cybersecurity revenue is expected to grow at an annual rate of 9.9% to $162.0 billion in 2023 with $85.5 billion coming from the security services segment and the rest from cyber solutions.[2] During the period 2023-2028, the market is estimated to grow at a compound annual growth rate (CAGR) of 9.6%, to a market size of $256.6 billion in 2028, according to Statista. This growth is expected to be led by the cyber solution segment with an estimated CAGR of 14.2% and a resultant market size of $148.7 billion in 2028 followed by the security services segment at a lower rate of 4.8% and a resultant market size of $107.9 billion in 2028.[3] Region wise, the largest market for cybersecurity, the U.S. is expected to have a market size of $68.7 billion in 2023, and is expected to grow at a CAGR of 8.5% during the period 2023-2028 to a market size of $103.4 billion by 2028.[4]
- According to Statista, cybercrimes are expected to cost about $8.2 trillion in 2023 with the cost expected to grow to $13.8 trillion in 2028.[5] In May 2023, Moody's Investors Service warned about credit risk from state-sponsored cyber attacks, particularly on sectors such as communications, utilities, energy and transportation.[6] A McKinsey report published at the end of 2022 predicted that the estimated addressable market in cybersecurity is a staggering $1.5-$2.0 trillion, with only ~10% of the market penetrated at current levels.[7]
- International law enforcement agencies, including the FBI and other European, Canadian, and Australian police organizations have taken down Genesis marketplace, popular with cybercriminals in a multinational crackdown dubbed "Operation Cookie Monster".[8] The site, according to Britain's National Crime Agency, hosted about 80 million credentials and digital fingerprints stolen from more than 2 million people.[9] The FBI was also able to take down Russia's premier cyber-spying tool called "Snake"; this was made possible through exposure of "Snake" by the Cybersecurity and Infrastructure Security Agency (CISA) which issued a joint advisory in May 2023.[10]
- The Securities and Exchange Commission (SEC) has proposed a new rule to tackle the risks posed by cyber threats to capital markets. The new rule, Rule 10, is the most recent one in a series of rules introduced by the SEC in 2022, to tackle cyber-related risks in capital markets. According to Reuters, if adopted, Rule 10 would require market entities to report cyber risks and incidents to the SEC on a "Form SCIR," part of which would be publicly available. Overall, the rule would help guarantee increased transparency into the inner workings of market entities and a better assessment of cyber-risks to the U.S. securities markets.[11]
- The United States and Europe continue collaborating with each other to tackle cyber threats. Recently, they launched a "cyber dialogue" to strengthen cooperation ahead of the Cyber Solidarity Act being proposed by the European Commission[12]. They have also issued a joint advisory to help organisations counter APT28, a threat group attributed to Russia's military intelligence service, which has been observed taking advantage of poorly configured networks and exploiting a known vulnerability to deploy malware and access Cisco routers worldwide.[13] Cybersecurity agencies in U.S., Australia, Canada, the U.K., Germany, the

Netherlands, and New Zealand have published new guidelines, based on the principles published by CISA, which urge manufacturers to build in cyber safety to their products at the design stage itself.[14]

- In Europe, Italian aerospace and defence group Leonardo and German technology company Siemens have signed a memorandum of understanding to offer cybersecurity solutions for infrastructure in the energy, oil and gas and industrial sectors.[15]
- Asia Pacific region is experiencing a higher rate of cyber attacks compared to its global counterparts, according to the World Economic Forum, fueled by factors such as accelerated digital transformation, hybrid working model, new generation of users and high manufacturing demand.[16]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q2 2023

- On June 12, Intellihartx, a company providing patient balance resolution services to hospitals informed 490,000 individuals that their personal information including medication information, birth dates, and Social Security numbers were compromised in the GoAnywhere zero-day attack earlier in February this year. The stolen data was made available on the the Cl0p ransomware gang's leak site.[17]
- On June 12, the Swiss government revealed that there was a cyberattack on May 23 on the technology firm Xplain, which provides software to several Swiss departments resulting in loss of operational data. The attackers posted some of the stolen data on the darknet. Xplain accused a ransomware group called Play of being behind the attack. The group published the entire stolen data on June 1 after it failed to receive the ransom amount.[18,19]
- On June 5, in a significant cyberattack, the Cl0p ransomware gang exploited MOVEit to steal data from several dozen organizations that later confirmed being impacted. Progress Software owns the MOVEit Transfer software, widely used by major businesses worldwide, to securely share files. The first cyberattacks involving MOVEit were noticed on May 27. Security researcher Kevin Beaumont claims data was stolen from several entities and government agencies and that 100 large entities were hit by the cyberattack. One victim is the UK-based payroll and HR company Zellis, whose customers included British Airways, the BBC, Irish airline Aer Lingus, and UK pharmacy chain Boots. The Cl0p ransomware syndicate announced on its dark website that victims had until June 14 to pay the ransom, failing which the data would be published online.[20,21,22]
- On June 3, one of Australia's largest law firms HWL Ebsworth, confirmed that its network was hacked on April 28 after the ALPHV/ BlackCat ransomware gang published 1.45 terabytes (TB) of stolen data and threatened to leak more if their demand of $4 million in cryptocurrency wasn't met. The gang is believed to have stolen 3.6 TB of data. The law firm stated firmly they do not intend to meet the demands of the ransomware gang even at the cost of leaked client data. HWL Ebsworth has several hundred clients including dozens of federal government agencies.[23,24,25]
- On June 3, a ransomware attack on Japanese pharma giant Eisai resulted in encryption of several of its servers, impacting their Japan and overseas operations. The company reported that they were yet to determine if any data was stolen.[26]
- On June 2, Point32Health, the second-largest health insurer in Massachusetts, started informing 2.5 million patients that their sensitive healthcare and personal information was stolen in a ransomware attack. The incident occurred on April 17 and impacted systems supporting its Harvard Pilgrim Health Care Commercial and Medicare Advantage Stride plans. The insurer was not aware if the data is being misused or of any ransomware gang claiming responsibility.[27,28]

- On June 2, biotechnology company Enzo Biochem (NYSE: ENZ) revealed that clinical data pertaining to 2.47 million individuals was exposed in a ransomware attack. The attack occurred on April 6 and the social security numbers of 600,000 patients may have leaked.[29]
- On May 30, dental benefits manager MCNA started informing 9 million individuals that their personal information may have leaked in a cyberattack earlier this year that occurred between February 26 and March 7. The LockBit ransomware group accessed multiple systems within MCNA's network, infected them with malware, and stole personal information. In April, the group published 700 gigabytes of data on its leak website.[30]
- On May 29, two eastern Idaho hospitals and their clinics were the target of cyberattacks, causing some clinics to shut down and some ambulances to be diverted to the nearby hospital. The hospital IT staff were prompt to identify the attack and limit the damage.[31]
- In the week of May 27, ABB (SWX: ABBN) confirmed that Black Basta ransomware group infiltrated its systems using malware and stole information. The company's factories were operating, and its forensic investigation found no evidence of customer systems being directly impacted. Though company officials refused to comment, Kevin Beaumont, a reputable cybersecurity researcher, confirmed that the ransom amount was paid.[32]
- On May 23, Rheinmetall (ETR: RHM), a German car parts maker and defense company was attacked by the Black Basta ransomware cybergang on April 14 which impacted its automotive business but not its defense business. The cybergang stole certain classified documents. The company was also the target of a malware attack in 2019 affecting its automotive plants in the U.S., Brazil, and Mexico.[33]
- On May 22, satellite TV provider Dish Network (NASDAQ: DISH) notified 296,000 employees and their family members whose data was compromised in a cyberattack. The incident occurred in late February 2023 when various services, including Dish websites and applications, became inaccessible. The company confirmed stolen data being deleted which suggests that the ransom amount may have been paid.[34]
- On May 22, technological equipment giant Lacroix Group (EPA: LACR) had to shut down three production sites after a cyberattack on May 12 hit its French, German and Tunisian sites that produce electronics systems. File-encrypting ransomware was deployed and some of the local infrastructures were encrypted.[35]
- On May 15, pharmacy network PharMerica (NYSE: PMC) sent notifications to more than 5.8 million individuals to disclose a data breach that occurred in March 2023. The pharmacy did not divulge the name of the attacker, but it appears that Money Message ransomware group is responsible for the attack. In April, the group started leaking personally identifiable information and protected health information allegedly stolen from PharMerica.[36]
- On May 10, industrial cybersecurity vendor startup Dragos revealed a ransomware group breached its defenses and accessed threat intel reports, a SharePoint portal and a customer support system but failed to gain control of a Dragos system and deploy ransomware. Dragos said it decided not to engage with the criminals and ignored all attempts at communication with them.[37]
- On May 8, California's San Bernadino county Sheriff's Department announced that it had made a ransom payment of $1.1 million for a ransomware attack. The county was investigating if any data was stolen in the attack.[38]
- On May 5, data storage company Western Digital (NASDAQ: WDC) issued a second public statement stating that cybercriminals stole customer information after a ransomware group known as Alphv/BlackCat started publishing screenshots showing the extent of their access. The actual breach

occurred on March 26 and on April 2 the company shut down some services as part of the incident response.[39,40]

- On April 17, U.S. payment giant **NCR** (NYSE: NCR) stated that a cyberattack on April 13 and the subsequent outage at a data center impacted a limited number of ancillary Aloha applications for a subset of its hospitality customers. BlackCat, Alphv and Noberus took credit for the attack on its Tor-based leak website, but the post was removed quickly by the hackers suggesting that both parties were negotiating on the ransom payment.[41]
- On April 10, Australian consumer lending company **Latitude Financial** revealed that hackers stole personal information of around 14 million Australian and New Zealand customers in March. The firm received a ransom threat but chose to ignore it in line with the government advice.[42]
- On April 10, Taiwan-based tech major **Micro-Star International,** MSI, (TPE: 2377) confirmed that a cyberattack disrupted its systems but it did not impact its financial business. A ransomware group 'Money Message' claimed to have accessed MSI's internal databases, private keys, source code, and BIOS firmware and demanded $4 million in ransom amount.[43,44]
- On March 31, **Capital PLC** (LON: CPI), one of the largest business outsourcing providers in the UK, issued a statement that it faced IT issues. Three days later, it announced that they were caused by a cyber incident. On April 20, the company confirmed that hackers accessed roughly 4% of its server infrastructure and stole files hosted on the breached systems. In a later update, the date of breach was identified as March 22. On April 17, the Black Basta ransomware gang posted on its extortion portal on the dark web threatening to sell the stolen data, if the ransom was not paid. On May 10, the company mentioned only 0.1% data was exfiltrated as against 4% mentioned earlier and that it expects to incur ~$19-25 million on the cybersecurity incident, but it's unclear if the amount also includes ransom payment.[45,46]

New Products

- Akamai Technologies (NASDAQ: AKAM) introduced a range of new products and updates in April 2023, which included the launch of updated managed security service programs and premium service offerings. According to the company, "the new capabilities are intended to help customers protect their businesses 24x7 from the most sophisticated attacks with proactive monitoring and rapid response in the event of a cyberattack."[47] It has introduced new cloud computing capabilities for streaming videos which primarily helps OTT operators to deliver higher quality and more personalized video experiences to viewers.[48] It has introduced Brand Protector, a new solution that detects and disrupts phishing sites, fake stores, and brand impersonations.[49] Akamai introduced Prolexic Network Cloud Firewall which "allows customers to define and manage their own access control lists (ACLs) while enabling greater flexibility to secure their own network edge".[50]
- Palo Alto Networks (NASDAQ: PANW) in May 2023 has introduced cloud next-generation firewall (NGFW) for Microsoft Azure customers. The product acts as a fully managed Azure-native ISV service. As per the company, "powered by AI and ML, the product can stop known, unknown and zero-day threats, enabling customers to safely and more quickly migrate their applications to Azure".[51] The company has also expanded its Unit 42's digital forensics and incident response service in April 2023. It claims that the product will "equip enterprises to respond immediately and recover faster than most any digital forensics and incident response (DFIR) service in the market".[52]
- BlackBerry Limited (NYSE: BB) in April 2023 has introduced the industry's first integrated solution that combines CylanceGUARD® and BlackBerry® AtHoc® technologies to assure secure bi-directional response

communications during cyber incidents.[53] It has also rolled out a revamped version of AI-based Cylance, which reduces alert fatigue by 90%, compared to previous versions and offers faster incident response, expands cloud defense coverage and makes organizations' zero trust network access adoption journeys easier.[54] In May 2023, the company announced the release of QNX software development platform 8.0 to enable automakers and IoT systems developers to deliver more powerful products at lower costs with heightened safety.[55]

- Cloudflare (NYSE: NET) in May 2023 launched its generative AI version of its single-vendor SASE platform, Cloudflare One. The product is a suite of Zero Trust security controls, which will enable enterprises to use generative AI tools without putting intellectual property and customer data at risk.[56]

Cybersecurity – M&A and IPO Activity in Q2 2023

Inside HUR Index Activity:

- On May 31, Cisco (NASDAQ: CSCO), announced its intent to acquire U.S.-based Armorblox, Cisco's third acquisition in 2023 in the cybersecurity space. Armorblox, founded in July 2017, has raised $46.5 million in four rounds of outside funding. The most recent round was led by SentinelOne's venture capital arm in September 2022. Armorblox's use of predictive and generative artificial intelligence (AI) across Cisco's portfolio will lead to enhanced attack prediction, rapid threat detection, and efficient policy enforcement. The deal value is undisclosed but IT-Harvest estimates that Armorblox is worth between $71 million and $97 million based on available funding and revenue of $11.4 million.[57,58]
- On May 16, Crosspoint Capital Partners agreed to acquire Absolute Software (NASDAQ: ABST) at $11.50 per share for a total enterprise valuation of $870 million. Excluding debt, the transaction is valued at $657 million. The deal is approved by Absolute's board of directors but is subject to shareholder and regulatory approvals. ABST provides security solutions that offer visibility and control over devices, applications, and network connections.[59]

Outside HUR Index Activity:

- On May 16, IBM (NYSE: IBM) announced a deal to acquire Israel-based Polar Security, an early-stage startup in the red-hot data security posture management space (DSPM) for $60 million. Polar had previously raised $8.5 million from Glilot Capital Partners in seed-stage funding. Its software helps organizations track, manage and secure identities and data flowing through cloud deployments.[60]

Venture Capital and Other Private Equity Activity:

- On June 9, Blackpoint Cyber raised $190 million in growth funding led by Bain Capital Tech Opportunities with participation from Accel. The firm, founded in 2014, provides an advanced security suite via managed service providers (MSPs). Blackpoint's Managed Detection and Response (MDR) technology identifies and isolates threats at the early stages of a breach and provides continuous monitoring via its security operations center (SOC).[61]
- On May 30, SGT Capital agreed to acquire Elatec in a deal valued at EUR 400 million (~$433 million). Elatec is a leading international developer and supplier of secure access management solutions. The firm's solutions combine essential elements of secure physical and cyber access for electric vehicle charging infrastructure, smart city, smart building, smart office, and operator access into one integrated internet of things (IoT) and software-as-a-service (SaaS) platform. The deal is subject to customary regulatory approvals.[62]

- On April 13, Cinven, a private equity firm, entered into an agreement to acquire Archer from RSA Security. Founded in 2000, Archer is a leading provider of governance, risk, and compliance (GRC) software globally. Archer serves more than half of Fortune 500 companies, with a highly recurring revenue stream, strong visibility, and high customer retention. Financial terms of the transaction were undisclosed. In January 2023 RSA Security was exploring a sale of Archer at a $2 billion-plus valuation.[63,64]
- On May 2, Sourcepass, an IT Services and Cybersecurity provider, secured $65 million in funding, bringing their total funding to $135 million. The funding supports the firm in its strategic objectives including the acquisition of Proxios which expands their physical presence in the mid-Atlantic states, while broadening their client base in the healthcare, legal, and non-profit sectors. The firm has plans to make strategic acquisitions increasing their vertical markets and hiring talent resources in 2023.[65]
- On April 21, Texas startup Halcyon secured $50 million in a Series A funding round from venture capitalists led by SYN Ventures, an investment firm that makes early-stage bets on cybersecurity companies, apart from equity investments from Dell Technologies Capital and Corner Capital. The firm is developing an AI-powered cyber resilience platform to protect companies from ransomware. The multi-tiered approach of Halcyon uses AI/machine learning (ML) engines to detect and block any known bad executables like off-the-shelf commodity ransomware and passes unknown but suspicious executables to the additional protection layers for further analysis.[66]

[1] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[2] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[3] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[4] https://www.statista.com/outlook/tmo/cybersecurity/united-states
[5] https://www.statista.com/outlook/tmo/cybersecurity/worldwide#cybercrime
[6] https://www.cybersecuritydive.com/news/moodys-credit-risk-cyber-critical-infrastructure/651656/
[7] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
[8] https://www.weforum.org/agenda/2023/04/cybersecurity-news-cyber-threats/
[9] https://www.weforum.org/agenda/2023/04/cybersecurity-news-cyber-threats/
[10] https://www.weforum.org/agenda/2023/05/cybersecurity-news-to-know-this-month/
[11] https://www.reuters.com/legal/legalindustry/sec-is-inching-closer-clarity-cybersecurity-requirements-2023-04-19/
[12] https://www.weforum.org/agenda/2023/04/cybersecurity-news-cyber-threats/
[13] https://www.ncsc.gov.uk/news/uk-and-us-issue-warning-about-apt28-actors-exploiting-poorly-maintained-cisco-routers
[14] https://www.weforum.org/agenda/2023/04/cybersecurity-secure-by-design-software-guidance/
[15] https://www.weforum.org/agenda/2023/04/cybersecurity-news-cyber-threats/
[16] https://www.weforum.org/agenda/2023/06/asia-pacific-region-the-new-ground-zero-cybercrime/
[17] https://www.securityweek.com/intellihartx-informs-490k-patients-of-goanywhere-related-data-breach/
[18] https://www.securityweek.com/swiss-fear-government-data-stolen-in-cyberattack/
[19] https://www.bleepingcomputer.com/news/security/swiss-government-warns-of-ongoing-ddos-attacks-data-leak/
[20] https://www.securityweek.com/ransomware-group-used-moveit-exploit-to-steal-data-from-dozens-of-organizations/
[21] https://www.securityweek.com/several-major-organizations-confirm-being-impacted-by-moveit-attack/
[22] https://www.securityweek.com/bbc-british-airways-novia-scotia-among-first-big-name-victims-in-global-supply-chain-hack/
[23] https://www.bleepingcomputer.com/news/security/blackcat-ransomware-fails-to-extort-australian-commercial-law-giant/
[24] https://www.oodaloop.com/cyber/2023/06/20/australian-government-says-its-data-was-stolen-in-law-firm-ransomware-attack/
[25] https://www.theguardian.com/australia-news/2023/jun/20/ndis-agency-scrambles-over-risk-of-leaked-sensitive-client-information-in-hwl-ebsworth-hack
[26] https://www.securityweek.com/pharmaceutical-giant-eisai-takes-systems-offline-following-ransomware-attack/
[27] https://www.securityweek.com/information-of-2-5m-people-stolen-in-ransomware-attack-at-massachusetts-health-insurer/
[28] https://www.securityweek.com/ransomware-attack-hits-health-insurer-point32health/
[29] https://www.securityweek.com/enzo-biochem-ransomware-attack-exposes-information-of-2-5m-individuals/
[30] https://www.securityweek.com/personal-information-of-9-million-individuals-stolen-in-mcna-ransomware-attack/
[31] https://www.securityweek.com/idaho-hospitals-working-to-resume-full-operations-after-cyberattack/
[32] https://www.securityweek.com/industrial-giant-abb-confirms-ransomware-attack-data-theft/
[33] https://www.securityweek.com/rheinmetall-says-military-business-not-impacted-by-ransomware-attack/
[34] https://www.securityweek.com/dish-ransomware-attack-impacted-nearly-300000-people/
[35] https://www.securityweek.com/lacroix-closes-production-sites-following-ransomware-attack/
[36] https://www.securityweek.com/pharmerica-discloses-data-breach-impacting-5-8-million-individuals/
[37] https://www.securityweek.com/dragos-says-ransomware-hackers-failed-at-elaborate-extortion-scheme/
[38] https://www.securityweek.com/1-1m-paid-to-resolve-ransomware-attack-on-california-county/

[39] https://www.securityweek.com/western-digital-confirms-ransomware-group-stole-customer-information/
[40] https://www.securityweek.com/leaked-files-show-extent-of-ransomware-groups-access-to-western-digital-systems/
[41] https://www.securityweek.com/payments-giant-ncr-hit-by-ransomware/
[42] https://www.securityweek.com/australian-finance-company-refuses-hackers-ransom-demand/
[43] https://www.securityweek.com/msi-confirms-cyberattack-issues-firmware-download-guidance/
[44] https://www.bleepingcomputer.com/news/security/money-message-ransomware-gang-claims-msi-breach-demands-4-million/
[45] https://www.bleepingcomputer.com/news/security/capita-confirms-hackers-stole-data-in-recent-cyberattack/
[46] https://www.securityweek.com/capita-says-ransomware-attack-will-cost-it-up-to-25-million/
[47] https://www.akamai.com/newsroom/press-release/akamai-launches-managed-security-service-updates-and-new-premium-offering
[48] https://www.akamai.com/newsroom/press-release/akamai-announces-new-cloud-computing-capabilities-for-streaming-video-at-2023-nab-show
[49] https://www.akamai.com/newsroom/press-release/akamai-announces-brand-protector-to-defend-against-phishing-attacks-and-fake-websites
[50] https://www.akamai.com/newsroom/press-release/akamai-introduces-prolexic-network-cloud-firewall
[51] https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-unveils-its-cloud-next-generation-firewall-for-microsoft-azure-customers
[52] https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-takes-aim-at-cyber-attacks-with-the-expansion-of-unit-42-s-digital-forensics---incident-response-service-globally
[53] https://www.blackberry.com/us/en/company/newsroom/press-releases/2023/blackberry-introduces-industry-first-integrated-solution-to-assure-secure-bi-directional-response-communications-during-cyber-incidents
[54] https://www.blackberry.com/us/en/company/newsroom/press-releases/2023/blackberry-delivers-more-security-less-complexity-with-enhanced-cybersecurity-solutions-portfolio
[55] https://www.blackberry.com/us/en/company/newsroom/press-releases/2023/blackberry-qnx-releases-ultra-scalable-high-performance-compute-ready-operating-system-to-advance-software-development-efforts-for-next-generation-vehicles-and-iot-systems
[56] https://www.cloudflare.com/press-releases/2023/zero-trust-security-to-safely-use-generative-ai/
[57] https://www.bankinfosecurity.com/cisco-buys-armorblox-to-bring-generative-ai-to-its-portfolio-a-22204
[58] https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/acquisitions-list-years.html
[59] https://www.securityweek.com/crosspoint-capital-partners-acquires-absolute-software-in-870-million-deal/
[60] https://www.securityweek.com/ibm-snaps-up-dspm-startup-polar-security/
[61] https://www.securityweek.com/blackpoint-raises-190-million-to-help-msps-combat-cyber-threats/
[62] https://www.prnewswire.com/news-releases/sgt-capital-acquires-elatec-the-leading-global-provider-of-secure-access-solutions-301836733.html
[63] https://www.prnewswire.com/news-releases/cinven-to-acquire-archer-301796617.html
[64] https://www.reuters.com/markets/deals/rsa-security-explores-2-bln-plus-sale-archer-sources-2023-01-18/
[65] https://www.prnewswire.com/news-releases/sourcepass-announces-135-mm-in-total-funding-and-their-7th-acquisition-proxios-301813664.html
[66] https://www.securityweek.com/halcyon-secures-50m-funding-for-anti-ransomware-protection-platform/

Disclaimer:

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.
© 2023. Nasdaq, Inc. All Rights Reserved.