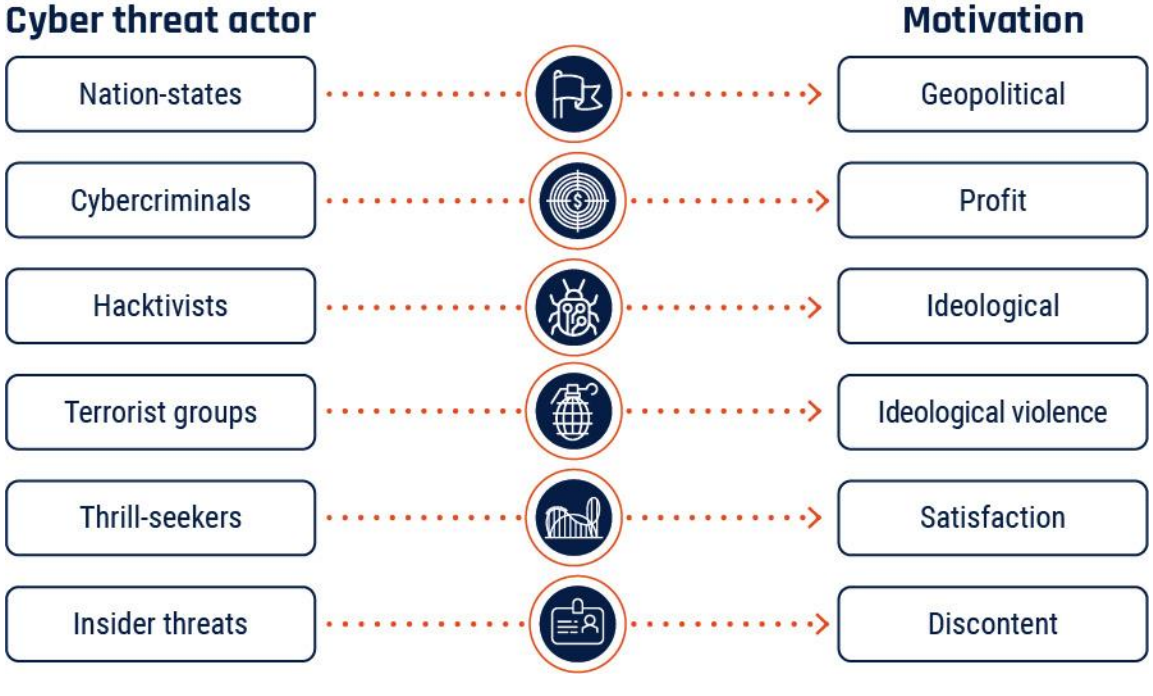
Highlights

Security Teams Focus on Latest Attack Trends, Not How They Are Likely to be Targeted

Posted by Karen Heumann, Febuary 16, 2023

Mandiant's Global Perspectives on Threat Intelligence report found that four out of five (79%) businesses make most cybersecurity decisions without insights into the threat actor targeting their infrastructures. Nearly half (47%) admitted that effectively applying that intelligence throughout the security organization was one of their most significant challenges, and nearly all (98%) said they need to be faster at implementing changes to their cybersecurity strategy based on threat intelligence. While more than 85% of security leaders appreciate the importance of identifying attackers, their tools and techniques, and motivations, only 34% said they consider the source of a potential attack when they test their cybersecurity defenses and admit to making purchase decisions based on latest attack trends.

Cyber threat actors and their motivations:



Mandiant commissioned a survey of 1,350 cybersecurity decision-makers at organizations with at least 1,000 employees, across 18 sectors in 13 countries to gain a global perspective on how organizations are leveraging threat intelligence to navigate the global cybersecurity threat landscape.

Other key findings:

- Cyber security is only discussed on average once every four or five weeks with various departments within organizations, including the board, members of the C-suite and other senior stakeholders. This cadence is even less frequent for groups such as investors, where the average lowers to once every seven weeks.
- Only 38% of security teams share threat intelligence with a wider group of employees for risk awareness.
- A majority (79%) of respondents relayed that their organization could focus more time and energy on identifying critical trends.

One of the problems highlighted by the survey is information overload. 84% of respondents said they were concerned that they may be missing vital threat intelligence due to the number of alerts and data they have to process, and 69% of respondents said they feel overwhelmed by the threat intelligence data they receive. In healthcare, 79% of respondents said they feel somewhat or completely overwhelmed by the amount of data and alerts they have to deal with.

Florida and South Dakota Decline Federal Security Funds; Nevada Needs Protection Most

Posted by Mike Heumann, Febuary 16, 2023

Florida and South Dakota are the only two states in the United States that declined to apply for federal funding to address cybersecurity issues. The State and Local Cybersecurity Improvement Act money includes $1B in grant money for state, local and territorial governments to defend themselves against cyberattacks. After $185M dispersed in the first year, $400M will be doled out in year two, $300M in year three, and $100M in year four.

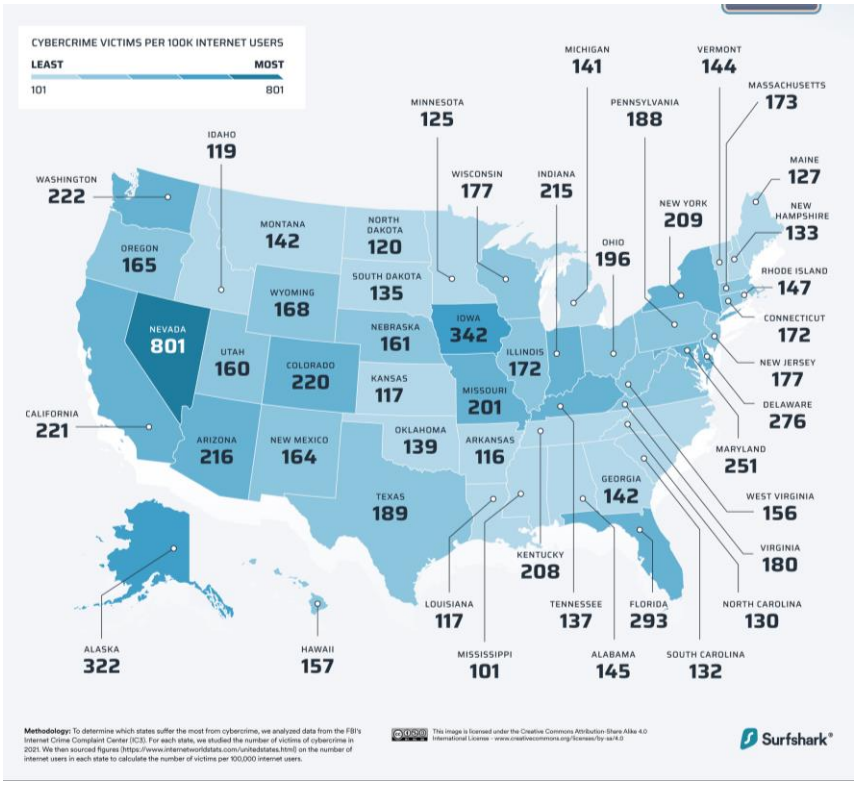
Florida officials object to "invasive and bureaucratic requirements" that will do little to enhance Florida's cybersecurity capabilities" in the funding application and state that the money is not needed because they offer a $30M grant program for local governments to strengthen their cybersecurity, increased pay for state cybersecurity employees, allocated $50M to improve cybersecurity resilience within state agencies, $30M for state and local government employee cybersecurity training, and $7M on a cybersecurity risk assessment of the state's critical infrastructure.

South Dakota representatives say their state has already allocated $30M for a cybersecurity applied research lab at Dakota State University. They also object to “substantial administrative burdens” and the current structure “only gives temporary funding.”

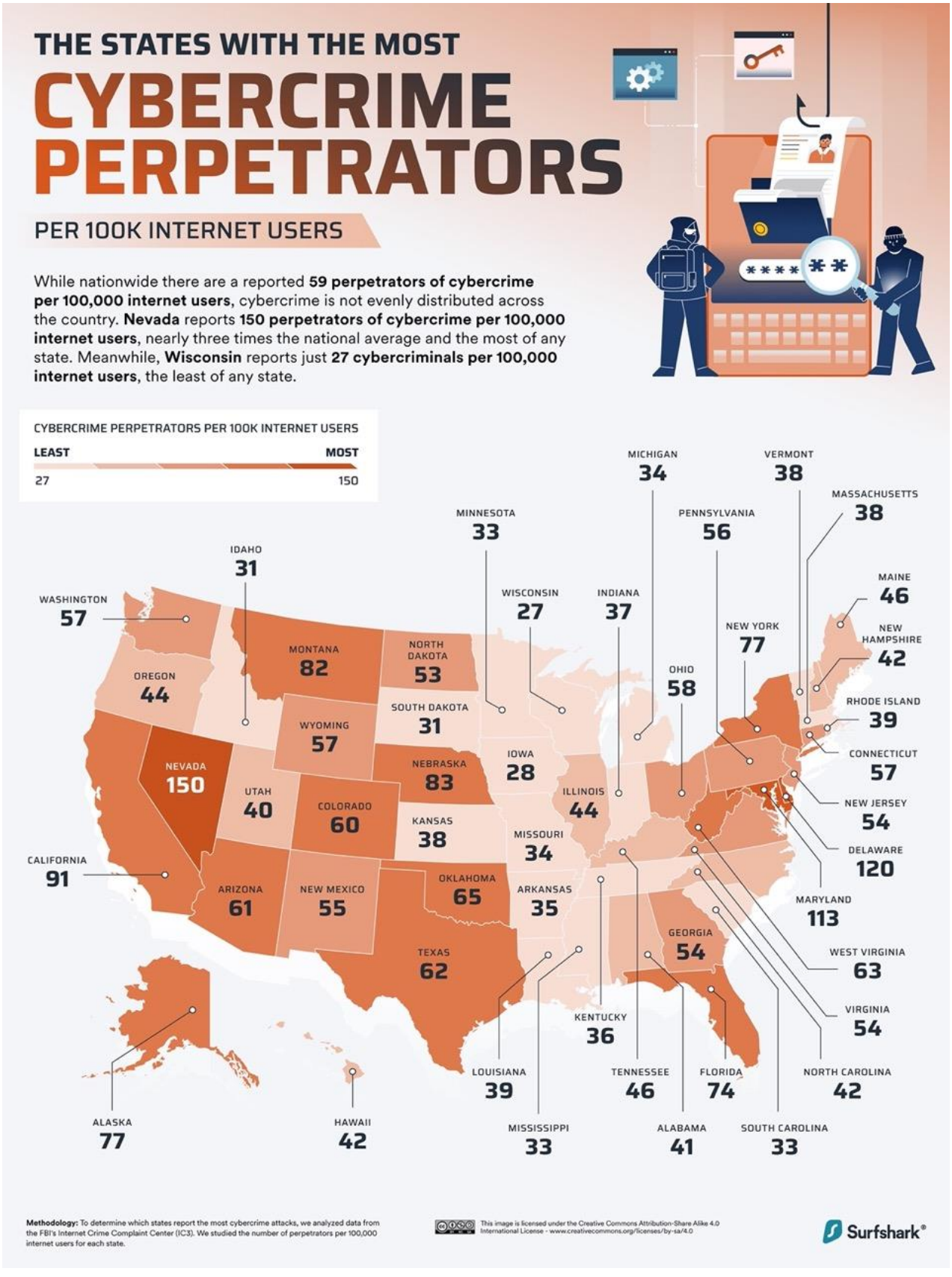
The ten states most at risk of cybersecurity attacks are Hawaii, Pennsylvania, Nevada, Florida, Wisconsin, Arizona, New Jersey, Alaska, Colorado, and Tennessee based on an analysis of FBI cyberattack data, states who report to the National Governor’s Association for spending on cybersecurity, and how safe each state’s election systems are. California is the most cyberattacked state which researchers attribute to the high population, large public sector presence, and tech-savvy citizens. Florida comes in second but only has about half the population of California.

Rank	State	Total victims (2021)	Financial loss (2021)	Average Loss per Victim
1	California	67,095	$1,227,989,139	$18,302
2	Florida	45,855	$528,573,929	$11,527
3	Texas	41,148	$606,179,646	$14,732
4	New York	29,065	$559,965,598	$19,266
5	Illinois	17,999	$184,860,704	$10,271
6	Nevada	17,706	$83,712,410	$4,728
7	Ohio	17,510	$133,666,156	$7,634
8	Pennsylvania	17,262	$206,982,032	$11,991
9	Washington	13,903	$157,454,331	$11,325
10	New Jersey	12,817	$203,510,341	$15,878

Per capita, Nevada has the most cybercrime victims with 801 cybercrime victims per 100,000 internet users in 2021.



In Nevada, there are 150 perpetrators of cybercrime per 100,000 internet users, by far the most in any state and more than five times the rate in Wisconsin, where there are 27 perpetrators per 100,000 internet users. Delaware (120) and Maryland (113) are the only other states with more than 100 perpetrators of cybercrime per 100,000 internet users. California and New York also appear in the top 10, with 91 and 77 perpetrators of cybercrime per 100,000 internet users, respectively.



The Band Plays On, On Titanic Twitter

Posted by Karen Heumann, Febuary 16, 2023

Peiter “Mudge” Zatko, Twitter’s former head of security, has a long list of allegations against his former employer including:

- Twitter leadership misled its board and government regulators about its security vulnerabilities, including some that could make Twitter susceptible to foreign spying or manipulation, hacking, and disinformation campaigns.
- Twitter does not reliability delete users’ data after they cancel their account, in part because they lose track of user information.
- Twitter misled regulators about whether it deletes data as required.
- Executives do not have the resources to determine how many bots are on the platform.
- Twitter allows thousands of its employees to access central controls without oversight.
- About half of the company’s 500k servers run on outdated software that does not support basic security features such as encryption for stored data or regular security updates by vendors.
- The company also lacks sufficient redundancies and procedures to restart or recover from data center crashes and even minor outages of several data centers at the same time could knock the entire Twitter service offline.
- Senior Twitter executives have been aiding the company in covering up serious vulnerabilities.
- One or more current Twitter employees may be working for a foreign intelligence service – based on specific evidence provided to Twitter by a US government agency.

Zatko’s complaint says he was aware of “multiple episodes” of Twitter being penetrated by foreign intelligence agencies or being complicit in threat to democracies. Recently, a former Twitter manager was convicted of spying for Saudi Arabia. Zatko attempted to apprise

Twitter's board about security issues and his efforts to correct them. Whistleblower Aid filed "protected, lawful disclosures" with the Securities and Exchange Commission, Federal Trade Commission, and Department of Justice on Zatko's behalf, requesting an investigation into his allegations.

A Twitter representative says Zatko was fired by Twitter in January for poor performance:

> "Mr. Zatko was fired from his senior executive role at Twitter in January 2022 for ineffective leadership and poor performance," the Twitter spokesperson said. "What we've seen so far is a false narrative about Twitter and our privacy and data security practices that is riddled with inconsistencies and inaccuracies and lacks important context. Mr. Zatko's allegations and opportunistic timing appear designed to capture attention and inflict harm on Twitter, its customers and its shareholders. Security and privacy have long been company-wide priorities at Twitter and will continue to be."

Zatko believes he was fired in retaliation for pressing Twitter to address these security issues. According to Zatko's disclosure, Parag Agrawal, Twitter's former chief technology officer who was made CEO after Jack Dorsey stepped down, went to great lengths to hide the security issues including:

- Agrawal repeatedly discouraged Zatko from providing a full accounting of Twitter's security problems to the company's board of directors.
- Agrawal and his team required Zatko to provide an oral report of his initial findings on the company's security condition rather than a detailed written account to create the false perception of progress on urgent cybersecurity issues.
- And, the team is alleged to have hired a third-party consulting firm to issue a report hiding the security issues.

Sen. Chuck Grassley, the top Republican on the Senate Judiciary Committee and an avid Twitter user commented on Zatko's disclosures:

> "Take a tech platform that collects massive amounts of user data, combine it with what appears to be an incredibly weak security infrastructure and infuse it with foreign state actors with an agenda, and you've got a recipe for disaster," Grassley said. "The claims I've received from a Twitter whistleblower raise serious national security concerns as well as privacy issues, and they must be investigated further."

Jack Dorsey hired Zatko to work for Twitter after a 2020 hack of Twitter accounts for then-presidential candidate Joe Biden, former President Barack Obama, Kim Kardashian, and Elon Musk. Zatko, was a well-known "ethical hacker" turned cybersecurity insider and executive who had held senior roles at Google, Stripe and the US Department of Defense, and who told CNN that he'd been offered a senior, day-one cyber position in the Biden administration.

Zatko findings regarding Twitter's security practices were characterized as "egregious deficiencies, negligence, willful ignorance, and threats to national security and democracy."

During his tenure for Twitter, Zatko learned "it was impossible to protect the production environment. All engineers had access. There was no logging of who went into the environment or what they did…. Nobody knew where data lived or whether it was critical, and all engineers had some form of critical access to the production environment."

Twitter says it uses automated checks to ensure laptops running outdated software cannot access the production environment, and that employees may only make changes to Twitter's live product after the code meets certain record-keeping and review requirements.

In 2010, the FTC filed a complaint against Twitter for its mishandling of users' private information and the issue of too many employees having access to Twitter's central controls. The complaint resulted in an FTC consent order finalized the following year in which Twitter vowed to clean up its act, including by creating and maintaining "a comprehensive information security program." Zatko alleges because of their failure to address vulnerabilities raised by the FTC as well as other deficiencies, Twitter has "anomalously high rate of security incidents," approximately one per week serious enough to require disclosure to government agencies. "Based on my professional experience, peer companies do not have this magnitude or volume of incidents," Zatko wrote in a February letter to Twitter's board after he was fired by Twitter in January.

"One of the big disappointments in the Facebook order violation case was that the FTC let executives off the hook; they should've been named. And if there's a violation here — and that's a big if — then I think the FTC should very seriously consider not just fining the corporation but also putting the executives responsible under order," stated Jon Leibowitz, former chair of the FTC, to CNN in an interview.

Elon Musk has accused Twitter of lying about the number of spam bots on its platform.

Alone among social media companies, Twitter reports its user numbers to investors and advertisers using a measurement it calls monetizable daily active users, or mDAUs. Its rivals simply count and report all active users; until 2019, Twitter had worked that way as well. But that meant Twitter's figures were subject to significant swings in certain situations, including takedowns of major bot networks. So Twitter switched to mDAUs, which it says counts all users that could be shown an advertisement on Twitter – leaving all accounts that for some reason can't, for instance because they're known to be bots, in a separate bucket, according to Zatko's disclosure. The company has repeatedly reported that less than 5% of its mDAUs are fake or spam accounts, and a person familiar with the matter both affirmed that assessment to CNN this week and pointed to other investor disclosures saying the figure relies on significant judgement that may not accurately reflect reality. But Zatko's disclosure argues that by reporting bots only as a percentage of mDAU, rather than as a percentage of the total number of accounts on the platform, Twitter obscures the true scale of fake and spam accounts on the service, a move Zatko alleges is deliberately misleading.

Zatko began asking about bot accounts in early 2021 and was told that the company didn't know how many total bots are on its platform. It appeared to Zatko that Twitter "had no appetite to properly measure the prevalence of bots," in part because if the true number became public, it could harm the company's value and image. Zatko explains that Twitter's policy toward fake accounts incentivized "deliberate ignorance" by undercounting spam accounts and providing bonuses to executives for growing the number of users on the platform, but not sniffing out bots. Experts on inauthentic behavior online say it can be difficult to quantify "bots" because there isn't a widely agreed upon definition of the term, and because bad actors constantly change their tactics. There are also harmless bots on Twitter (and across the internet), such as automated news accounts, and Twitter offers an opt-in feature to allow such accounts to label themselves as automated. The company says it regularly challenges, suspends, and removes accounts engaged in spam and platform manipulation, including typically removing more than one million spam accounts each day. Twitter said the total number of bots on the platform is not a useful number.

"Twitter leadership is misleading the public, lawmakers, regulators and even its own board of directors," Peiter Zatko testified during a Senate Judiciary Committee hearing. "The company's cybersecurity failures make it vulnerable to exploitation, causing real harm to real people. "By going public, Zatko says, he believes he is doing the job he was hired to do for a platform he says is critical to democracy. "Jack Dorsey reached out and asked me to come and perform a critical task at Twitter. I signed on to do it and believe I'm still performing that mission," he said.

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

January 31 Pliops XDP-RAIDplus launch webinar featured Tony Afshary, Vice President, Products and Marketing at Pliops; Tom Sanfilippo, Chief Technical Officer at Paperspace (a Pliops XDP-RAIDplus user) and Yuyang Sun, Strategic Planner at Solidigm (a Pliops partner) on the value XDP-RAIDplus provides them. Pliops XDP-RAIDplus is the best-in-class protection solution for NVMe™ and NVMe-oF™ environments. This award-winning data protection solution overcomes the limitations of conventional RAID controllers with emphasis on data protection and resiliency, enabling higher endurance and usable life, reducing build times, and unlocking the capacity of high-density enterprise SSDs. The webinar video is available to view and a copy of the slidedeck is available here.

Interested in Sponsoring a webinar? Contact **G2M** for a prospectus. We can create custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Cybersecurity

Cybersecurity for Remote Workers & Mobile Devices	March 23
The Increasing Complexity of Cybersecurity Regulatory & Compliance for the Financial Services Industry	May 25
xDR- The Promise versus the Reality	August 3
10 Features of an Effective Attack Surface Management Tool	September 7
How Secure is the Cloud for Your Workloads?	October 12
Do You Need a SIEM? Use Cases Where a SIEM Makes Sense.	November 9

Enterprise Storage & Technology

The Need for Speed: NMVe, NVMe-oF, & Data Processing Accelerators	February 21
Supercharging Oracle MySQL Performance, Scalability, & Efficiency with Pliops	March 21
Storage Architectures for Artificial Intelligence & Machine Learning	April 4
Software-Defined Flash Memory Architectures	May 9
Storage & Compute Architectures for Healthcare & Imaging Applications	June 27
NVMe & NVMe-oF – Past, Present, & Future	July 11
GPUs, SSDs, & Shared Memory: Accelerating Computing?	August 22
Securing Data – How Storage & Cybersecurity Technologies Can Work Together	Sept 26
The Open Compute Platform (OCP) Movement – Providing Compute-At-Scale Value to On-Premises Deployments	October 24
Storage Architectures for HPC Clusters	November 21
2024 Trends – Cloud, On-Premises, & Hybrid Compute/Storage	December 12

Upcoming Conferences

February 27-28	Gartner Security & Risk Management Summit, Dubai
February 27-March 2	Mobile World Congress Barcelona
February 28-March 2	Rice University Energy HPCC Conference, Houston, TX
March 8-9	CloudExpo Europe, London
March 14-16	Gulf Information Security Expo, Dubai, UAE
March 20-22	Gartner Data & Analytics Summit, Grapevine, TX
March 20-23	GTC CPU Technology Conference, San Jose, CA
March 28-29	Gartner Security & Risk Management, Sydney, Australia
March 28-31	ISC West, Las Vegas
April 5-7	IST Information Security Expo, Tokyo, Japan
April 15-19	NABShow, Las Vegas
April 17-21	HIMMS Global Health Conference, Chicago, IL
April 17-21	Privacy Symposium, Venice, Italy
April 19-20	CyberSec Europe, Brussels, Belgium
April 24-27	RSA Conference, San Francisco
May 1-3	IAHSS AC&E, Nashville, TN
May 2-4	ACT Expo, Anaheim, CA
May 9-12	Black Hat Asia 2023, Singapore

May 15-17	Forth Roadmap Conference, Portland, OR
May 16-17	SIA GovSummit, Washington DC
May 21-25	ISC, Frankfurt, Germany
May 22-25	Dell World, Las Vegas
May 22-25	Government Fleet Expo, Dallas, TX
June 2-6	School Transportation Network Expo East, Indianapolis, IN
June 4-8	Cisco Live, Las Vegas
June 5-7	Gartner Security & Risk Managemnt, National Harbor, MD
June 7-9	Synnex Red, White and You, Greenville, SC
June 11-14	36th Electric Vehicle Symposium & Expo, Sacramento, CA
June 14-16	Interop Tokyo, Chiba, Japan
June 20-22	HPE Discover, Las Vegas
June 20-22	Info Security Europe, London
July 14-19	School Transportation Network Expo, Reno, NV
August 5-10	Black Hat USA, Las Vegas
August 8-10	Flash Memory Summit, Santa Clara, CA
August 28-31	VMWare Explore, US, San Francisco, CA
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX