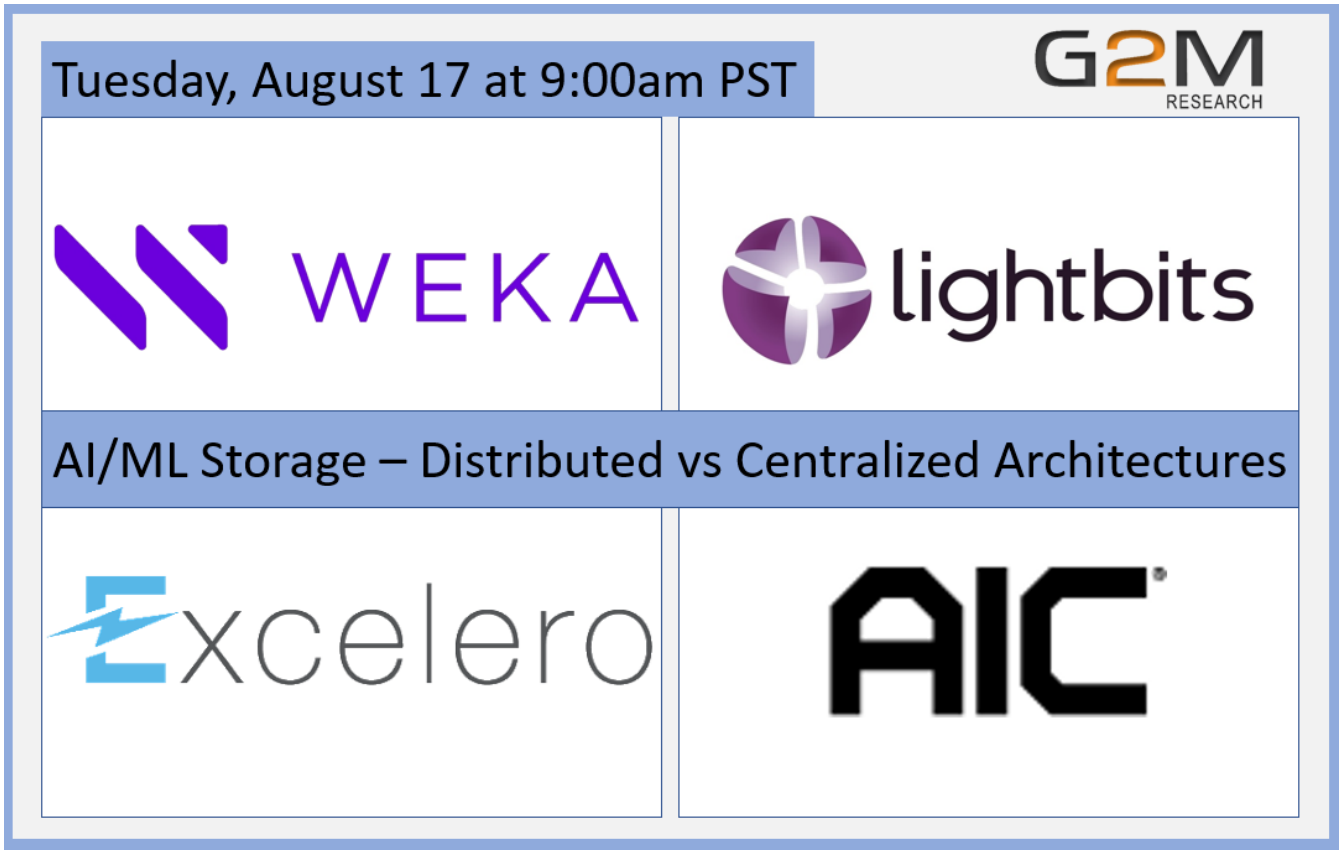
Highlights

Over 1300 people registered for our July 13 webinar, “Computational Storage vs Virtualized Computation/Storage in the Datacenter – And The Winner Is?” sponsored by ScaleFlux, Achronix, and Pliops. We have a handful of webinars left for 2021, we expect to schedule a couple of custom webinars, and our 2022 webinar schedule will be out soon – let us know how we can help you.

A list of upcoming AI & Cybersecurity events and links to register is below. Also, at the end of our newsletter, we include video of Daniel Camarena, the Padres relief pitcher, hitting his first major league hit – a grand slam – along with some interesting facts about the records broken in that game. What does this have to do with cybersecurity? Nothing. Great video, though.

Cheers! Mike Heumann



Lumen Technologies Predictions Provide Cybersecurity Roadmap

LUMEN®

Companies have to predict the future in order to prepare products and services to meet the needs of their current and desired customers. It is often a best guess and, perhaps, largely based on what is happening today – but at a greater magnitude. Yet, it seems that CSW interviewed some of the more prophetic of the cybersecurity industry, particularly as provided in the responses from Wai Kit Cheah, Director, Security Practice at Lumen Technologies. Each prediction below is evidenced at wide scale in the state of cybersecurity for 2021 and provide insight for companies to embrace to fend off these predictable hazards.

Remote Work Risks "With remote work, employees are no longer within the safety and confines of their corporate network. In a home environment, they would not be protected from malicious websites, drive-by downloads, malvertisements, as they would be in their corporate network behind security policies and protection layers. Chances are much higher that endpoints could inadvertently download a malicious malware or be infected with ransomware."

In February 2021 there were 377.5M brute-force attacks worldwide compared to 93M at the beginning of 2020.

Securing Critical Infrastructure "OT (Operational Technology) security is starting to be a concern especially to critical infrastructure operators, utilities, energies, heavy industries, large manufacturing, etc. We may not reach that danger point yet, but with the increasing digitization of the industries, potentially, this can be a national risk. Imagine the threat of a fire storm. Hijacked power plant, utilities grid, total black out. That may be a reality in 3 to 4 years' time if people don't start paying attention to securing their OT networks and infrastructure."

In May, a ransomware attack on Colonial Pipeline by hacking group DarkSide crippled gas and jet fuel supplies to nearly half the east coast. The pipeline is 5,500 miles long and can carry 3M barrels of fuel each day. Colonial Pipeline paid $4.4M in ransomware to prevent a longer shutdown of services (full article in our May AI & Cybersecurity Newsletter).

In February, a hacker gained access to a water treatment facility in Florida and attempted to raise the levels of sodium hydroxide (lye) in the water to lethal levels. An employee, monitoring the system, noticed the breach in time to avert the crisis.

On June 9, 2021, Cybersecurity & Infrastructure Security Agency (CISA) published Rising Ransomware Threat to Operational Technology Assets, a fact sheet for critical infrastructure owners and operators detailing the rising threat of ransomware to operational technology (OT) assets and control systems.

Zero-Trust Architecture "In my opinion, in the past, many of the larger enterprises focus much on threat modeling, threat intelligence, and analytics. Too much effort was spent on trying to understand the TTPs of bad actors out there. It is constantly evolving and changing. Often, that's like trying to keep up with a bullet train going at 300km/h. What's the alternative? I feel the alternative is slowly moving toward a zero-trust architecture. This is probably in the near future."

In our June AI & Cybersecurity newsletter, we highlighted predictions from Macy Dennis, CSO of Evotek, who also projected a move to the Zero Trust model ("By 2020 the majority of leading IT platform vendors, as well as cyber security providers, have well-documented examples of zero trust architectures or solutions.") This increased popularization has in-turn created a range of definitions of zero trust, requiring a level of standardization by recognized authorities such as NCSC and NIST.

Cybersecurity Awareness Training “Companies will start paying attention to cybersecurity awareness training. They will still find ways to conduct the training but will remain price-sensitive in spending. Some will just treat it as just a chore, a tick-in-the-box for compliance sake.”

> Mimecast reports that employees who receive regular awareness training are 5.2 times less likely to click on risky links than those without, yet their recent *State of email security* report shows only 19% of organizations provide ongoing cyber awareness training.
>
> Laurence Pitt, Director, Security Strategist at Juniper Networks, says security training is often dull, corporate, and unrewarding. He suggests, “Make the training fun. Humans learn better from positive rewards than negative experiences. An additional benefit is that people share something they enjoy, and so may pass on awareness tips to colleagues, family and friends. “Give virtual badges for completion of training, perhaps create a scorecard based on how quickly employees complete their training once assigned. Avoid rewarding right answers or time to complete the task.”

Critical Talent Shortfall “It will be harder to hire talent/skilled cybersecurity resources with the travel restrictions. Especially in smaller countries. Like in Singapore, we can only hire locally available candidates and you will see these people being poached every 6 months or so from one company to another. Many organizations will struggle to find the resources they need.”

> In the weeks before the Colonial Pipeline attack, the company had posted a job listing for a cybersecurity manager. The US Bureau of Labor Statistics projects "information security analyst" will be the 10th fastest growing occupation over the next decade, with an employment growth rate of 31% compared to the 4% average growth rate for all occupations.
>
> According to a 2020 industry survey there were 879,000 cybersecurity professionals in United States with a need to fill another 359,000 cyber jobs. The shortage is even greater globally with an estimated 3.12 million unfilled cyber jobs worldwide. Vacant positions range from entry-level to executive-level positions.

Increased Bot Risks “Web based applications will be at risk, especially if they have not adopted security design principles. Many home-brewed or in-house built web or mobile applications do not have basic controls in place. No input validations, no sessions time-out, allowing multiple concurrent logins, susceptible to various forms of attacks. Easy pickings.”

Ransomware Cyber-crime Fueled by Commission Criminals “You will see increased ransom based or financially motivated cyber-crime. Nowadays, there are many cybercrimes syndicate offering tools and services for hire (sometimes with guaranteed results) where they take a certain percentage of the

rewards. It makes it increasingly easier to partake in cyber-crime. Some examples include ransom-based DDoS threats on verticals like gaming or stock exchanges, as well as very targeted BEC attacks."

> From https://www.darkreading.com/vulnerabilities---threats/cybercrime-goes-mainstream/a/d-id/1340012: With revenues estimated up to $1.5 trillion a year — on average, 1.5 times more income than counterfeiting and 2.8 times more than the illicit drug trade — the cybercrime network is an economic system that can now threaten any company or organization and jeopardize the global economy. Roughly 60% of its massive revenues are estimated to come from illegal online markets for stolen data and 30% from pilfering intellectual property and trade secrets. Interestingly, only 0.07% is derived from ransomware, which inflicts the most real-world damage.

Skills Gap + Human Error Will Results in Increased Misconfigurations "Misconfigurations will continue to increase in magnitude. As companies get digitized and move into an online business model, adopt more cloud services, there will be more misconfigurations and mistakes made. Whether misconfigurations of cloud services, e.g. exposing an AWS s3 bucket to the whole wide world to see, or having an any-to-any default posture on firewalls, or exposing a database to the public. Partly human mistakes, partly stress, and also partly skills gap."

Compromised Network Access "Some consider insider threats as malicious employees. I think there is more to it than just employees. With compromised networks, a bad actor could infiltrate into a companies' network, install RAT, recon, move laterally, without being detected, especially if the security monitoring and posture of that organization is weak. In the dark forums, I believe there are compromised network access being sold for as low as a few hundred dollars. Behavioral-based monitoring and analytics will have increasing focus and might even become an accepted mainstream security monitoring mandate."

> Gurucel UEBA was recently awarded the 2021 Fortress Cyber Security Award for Most Advance Analytics. They analyze volumes od data generated by user and entity activity from the network, IT systems, cloud platforms, applications, IoT, endpoints and links thousands of discrete events to identify relationships to derive risk prioritized alerts for early detection, prediction, and prevention of threats from malicious insiders, fraud, account compromise, ransomware, and APT/stealth attacks that lay dormant between stages of a cyberattack

Data Leak Protection Means Understanding What You are Trying to Protect "With increasing penalties on data theft, and stricter PDPA/laws, executives and Board of Directors will pay more attention to data security. They might approve investment on DLP. But while the need for DLP may increase, I see a problem – DLP is just the technology part of the solution. To prevent data leakages requires a company to understand what data it is trying to protect. The solution is more of policies and

processes than technology. If a company does not even have data classification and the right policies, does not understand what they are trying to protect, then buying a DLP solution is not going to help at all. Many companies today do not even know what the critical assets are they collect, store, process, and manage, and have no idea where these data assets reside. You can't solve this gap by buying software."

Remote Work Creates Opportunities for Imposter Employee Communications "Working remotely changes the nature of how we operate. Our colleagues are not longer sitting next or near to us anymore. We can't turn around and ask our colleague, 'hey did you request for the approval of this transaction or payment?'. This is not possible anymore. Many, if not most, instructions will be coming through emails and sometimes in unsanctioned social messenger or communications platforms. It is crucial to train employees to be aware of the signs of social engineering, phishing, vishing, and always verify requests especially if it is a request for fund transfer or approval of a payment or critical transaction. This requires a new behavior, a new way of working."

> Businesses and individuals exchange more than 300 billion emails each day. Cybercriminals stole over $28 billion through email fraud from 2016 to 2020, with an average loss per incident of more than $150,000. A late 2020 survey by the Association of Certified Fraud Examiners, more than 80% of respondents across different organization types had observed an increase in cyber fraud since the pandemic began. This included business email compromise and payment fraud.

You Get What You Pay For "Many companies treat IT departments as a cost center. I've seen companies with more janitors and receptionists than IT personnel. Unfortunately, this translates to many unpatched systems and networks. As the IT teams scrambled to set up VPN for employees to work remotely, they often fail to validate if these VPN gateways are patched or have any critical vulnerabilities. Sometimes, these IT teams are inexperienced and are not aware of best practices. Many of these companies will have revenue and profit impact and in cutting costs, they will reduce spend. Some will do less in security, e.g. So, I predict that there will continue to be many more compromised networks and many more incidents of data breaches for most of 2021."

Wai Kit Cheah

Director, Security Practice

Lumen Technologies

Human Factors and Cybersecurity

Steve Durbin, Managing Director of the Information Security Forum (ISF), explains that "Cybercriminals have a deep understanding of human psychology and stress-related pandemic issues. In 2020 alone, Google registered a record two million phishing websites whereas ransomware attacks increased by sevenfold."

Some of the obstacles to security sound organizations, related specifically to people and not the technology, include the disruption of following secure protocols, the perception that security personnel fit a certain model with specific coding and computer science backgrounds, an organizational culture that does not invite or encourage critical thinking, treating every job and person as having the same needs, and investing in training that embraces participation and reinforce desired security outcomes.

While companies invest in security via their IT department, Durbin stresses the critical failings of such a shortsighted approach to preventing cyber breaches, and explains in numerous articles the need to address the entire organization, specifically the human factors aspect of cybersecurity. We highlight some quotes from his, Security of the Workforce, ISF Podcast:

"There's one thing that never changes and that is your ability to correctly predict how people behave. So many people have tried, and many people have failed. And, many people will continue to follow that same road, and I think that from this security standpoint, if you look at what security tries to do, security loves things that are predictable – things that it can anticipate, ideally. And, so people fit outside that realm. And, you hear a lot about zero trust, and all that kind of thing, is the way to go from a security standpoint, but you can't apply that to people. So, if you zero trust any of your people then you might as well pack up and go home. You have no business. And, of course, you know zero trust doesn't mean that you don't trust. It just means that you make an assumption that something that can go wrong, will go wrong. But, even then, within a people environment that does work well. It doesn't sit well with my view of a trusting culture, a flexible culture, a culture that has a broad mix of generations that's highly diverse, that's agile,

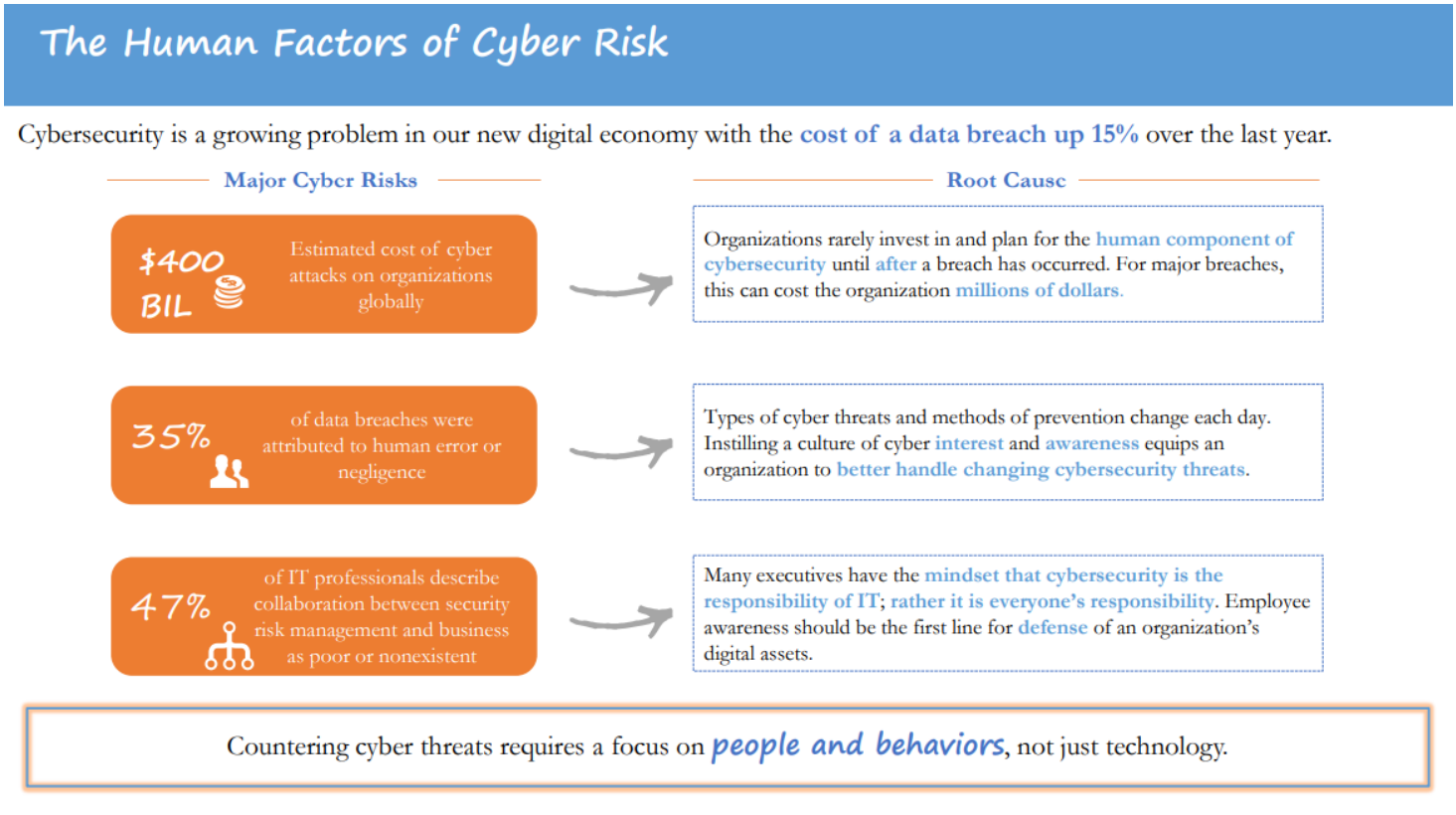
Steve Durbin
Managing Director, ISF

that encourages people to question, to challenge. Because that's how you build a thriving business, in my view."

"For me, everything begins and ends with people. Even if you introduce a high degree of artificial intelligence and machine learning into your processes, you will still have to deal with people, in some way, shape, or form. It's a constant and that's why I keep coming back to it. Because, we haven't cracked it. I don't think we ever will. And, I think we have to keep working at it."

"If you're going to have security being recognized as adding value to your business, then you have to move away from a reliance on pure technology to get your message across, so you have to be able to articulate the value that you bring to the business – not just in the boardroom but in every single department that you touch. And, so an understanding of the way people operate, the way that people take on board messages, the way that they like perhaps to be involved, understanding the dynamic of an organization becomes increasingly more important."

47% of IT professionals describe collaboration between security risk management and business as poor or nonexistent. Many executives have the mindset that cybersecurity is the responsibility of IT; rather it is everyone's responsibility. Employee awareness should be the first line for defense of an organization's digital assets. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf



Pay Ransom?

Expect to Pay Again

As we know, ransomware attacks are on the rise and the ransoms are getting higher. In the first half of this year, there were more than 226.3M attacks. Of course, the real number is unknown and companies and insurance companies go to great lengths to avoid report of the breach.

Yonatan Streim-Amit

cybereason®

Ransomware criminals are now, not only attempting to extract money from their victims, but coming back a second time to extort more. Yonatan Striem-Amit, CTO and co-founder of Cybereason, explains, “Ransomware cybercriminals are constantly innovating on better ways to get companies to pay more. We’ve seen a shift as ransomware groups adopting nation-state and APT-style technologies to encrypt whole networks, employing both zero-day and lateral movement techniques. And we’ve seen that evolve even further into double extortion.” And, companies that pay find that much of the data they recover is corrupted.

FBI Director Christopher Wray says the cyber threat "is increasing almost exponentially." The FBI director added that the federal government is currently investigating "100 different ransomware variants, and each of those 100 has dozens, if not hundreds of victims."

Cybereason conducted a global study of nearly 1,300 security professionals and found more than half of organizations had been the victim of a ransomware attack, and 80% of businesses that paid the ransom demand suffered a second ransomware attack — often at the hands of the same criminals. At least one report forecasts the cyber insurance market value will hit $24.19 million by 2025. But, if you buy it, don’t advertise it because that, too, invites attacks. Cybercriminals prefer a victim with deep pockets.

The Ransomware Task Force is a private-sector led, 60-member organization that includes dozens of private companies along with the FBI, U.S. Cybersecurity and Infrastructure Security Agency (CISA), and other law-enforcement groups. The Task Force provides a 48 step framework to avoid cyber attacks with four priority goals: 1) to deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; 2) to disrupt the ransomware business model and decrease criminal profits; 3) to help organizations better prepare for ransomware attacks; and 4) to respond to ransomware attacks more effectively. Cisco is a founding member. Their Talos Intelligence group participates in cyber attack panels to advise companies and their insurance providers during an attack.

In 2020, one of the largest providers of phishing training, Knowbe4 reported that 17K organizations used their solutions to provider 9.5M phishing security test emails to 4M users – and if they failed the test, they received more security training. Probably good to test and to add training for those who need it BUT you also risk alienating good employees.

Therefore, experts recommend:

1) Test teams, not individuals.
2) Don't embarrass anyone.
3) Use fun/creative ways to teach security protocols including team competitions, rewards, positive reinforcement.
4) Coach underperforming teams.
5) Celebrate improvement in everyone.

KnowBe4

Intel Hardware Shield Technology

intel®

The Intel® Evo™ vPro® platform experience is designed with mobile workers in mind for responsiveness including an immersive visual experience, faster video and photo editing, instant wake, and all-day battery life.

With the latest Intel vPro mobile platform, Intel Hardware Shield delivers more technology to help ensure defense in depth. This technology is designed to help shut down an entire class of attacks that long evaded software only solutions. Intel also delivers the industry's first silicon-enabled AI threat detection to help stop ransomware and cryptomining attacks.

Responsive and Efficient Storage Architectures for CSPs

with sponsors NVIDIA, Excelero, & Pliops

What is your organization's greatest concern when using cloud storage? (select one):

Overall Cost:	15%
Cost Predictability:	12%
Performance:	12%
Performance Predictability:	15%
Security/Data Privacy:	31%
Other Concerns:	8%
No concerns/no opinion:	8%

When building a cloud datacenter's storage infrastructure, what is your greatest concern? (select one):

Scalability:	17%
Storage performance:	25%
Minimizing CPU utilization:	4%
CapEx/upfront costs:	17%
Avoiding vendor lock-in:	25%
Other:	0%
No opinion:	13%

G2M Research Multi-Vendor Webinar Series

Our webinar, Tuesday, July 13 “Computational Storage vs Virtualized Computation/Storage in the Datacenter – And The Winner Is?” sponsored by ScaleFlux, Achronix, and Pliops is available to view. Register for our webinars and we will send these recordings directly to you. Over 1300 registrants for this webinar!

View the recording here and/or download a PDF of the slides. Our webinar schedule is below- Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact **G2M** for a prospectus.

You can view all our webinars and access slide deck presentations.

G2M RESEARCH

Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Composable Infrastructure vs Hyper-Converged Infrastructure for Business Intelligence
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion

AI & Cybersecurity Events

July 16-17	The Diana Initiative
July 19-21	ISC West
July 19-22	International Conference on Cyber Security (ICCS)
July 21	Virtual DC Metro Cyber Security Summit
July 29-31	Ransomware Live
July 31-Aug 5	Blackhat 2021
July 31-Aug 13	Ringzer0: Virtual Vegas
Aug 2-4	Techno Security & Digital Forensics Conference Colorado
Aug 3-14	SANS Security Awareness Summit & Training
Aug 4-5	Gartner Data & Analytics
Aug 15-19	CRYPTO 2021
Aug 17-18	ISMG Virtual Cybersecurity Summit: Fraud & Payments Security
Aug 17-19	WorldFestival
Aug 17-19	Ai4 2021
Aug 19	FutureCon Overland Park
Aug 23-25	AcceleRISE

Just because…. July 8, Camarena, a relief pitcher, playing his second major league game ever, first career hit, Padres down 8-0 in the fourth, when Camarena stepped up to bat with 2 outs and bases loaded.

The southpaw nailed it with a grand slam that ultimately contributed to the Padres 9-8 victory. Did I mention that he was the relief pitcher, 2 outs, with 2 strikes?

Camarena became the second pitcher in Padres history with a grand slam, joining Mike Corkins (Sept. 4, 1970). Camarena is also the first relief pitcher from any team to hit a grand slam since Don Robinson on Sept. 12, 1985, for the Pirates against the Cubs.

The only other pitcher in National League or American League history to record his first hit via a grand slam was Bill Duggleby who went deep on April 21, 1898 with the Phillies.

It also was the first time Scherzer allowed a home run with a pitcher at the plate. The eight-run comeback tied the biggest comeback win in Padres history. #slamdiego