G2M RESEARCH

AI & CYBERSECURITY NEWSLETTER

JUNE 2021

Highlights

JBS Pays $11M to End Ransomware Attack

Teamsters Refuse to Pay Ransom

EVOTEK Cybersecurity Predictions – Hit or Miss?

AI & Machine Learning in Neurology

Poll Results – How to Take a 360 Degree View of Cybersecurity

Check out the lengthy list of upcoming AI & Cybersecurity events at the end of this newsletter. Even as in-person conferences are coming back, virtual conferences still remain attractive. Virtual conferences are an extremely cost-effective way to engage a worldwide audience of prospective customers, especially in light of global travel restrictions. The time and cost savings of attending multiple virtual conferences in any given week means higher engagement rates for these venues. For smaller companies and startups, being at a large show can be costly and challenging.

Our multivendor webinars hit those same strengths - Vendors engage hundreds of prospects at a substantive level. With multivendor format, they have conversations that feel spontaneous and engage in a deep dialogue with each panelist having a solid opportunity to argue their perspective. The high-quality recorded webinar and slide deck remain available for use long after the event. If you are interested in sponsoring a webinar but don't see a topic that quite fits your needs, we can modify topics or add topics to meet your objectives. Our entire webinar schedule is at the end of our newsletter

Would you really want to invite more air travel given [recent passenger behavior](#)? Airlines are reducing alcohol service accordingly…

Cheers! Mike Heumann

JBS pays $11M to End Ransomware Attack

JBS is the leading meat processor in the United States, supplying 20% of US beef, pork, and poultry. In September, OSHA fined JBS $15k after six workers died and 300+ workers tested positive for the COVID-19 at their Greeley, Colorado plant. In October, JBS paid $280M fine to resolve bribery charges. And, this month, JBS paid $11M in ransom to end a recent ransomware attack.

OSHA fined JBS $15k for failing to protect the 3000 workers at the Colorado plant. United Food and Commercial Workers Union Local 7 (UFCW 7) expressed disgust at the paltry fine, saying in a press release, "Please note ironically, that the OSHA bureaucrats are not working from this office because it is deemed too dangerous during the pandemic, while JBS' workers were not protected and six of our members died, amost 300 were infected." In March, JBS was ordered to pay several million dollars by Brazil courts in relation to contamination issues regarding lack of COVID-19 safety protocols, resulted in court ordered closing of three local JBS plants last year.

UFCW International President, Marc Perrone released the following statement, including the following excerpt:

"Since the beginning of the pandemic, meatpacking workers and UFCW have led the fight for better personal protective equipment, universal COVID-19 testing, better social distancing in plants, and the real and enforceable health and safety standards needed to keep these facilities safe. We have done our job, and all we have asked is that the federal government do it job and hold irresponsible employers accountable. This 'so-called fine' proves that this administration is incapable and unwilling to fulfill its duty to keep workers safe."

In October, JBS was fined over $280M by the Justice Department and Securities Exchange Commission for violating federal anti-corruption laws. Specifically, JBS used fund obtained through a bribery scheme to expand US operations. This violation is on top of the company admitting they used $150M to bribe officials in Brazil to obtain financing for additional expansion, and paid fines over $3.2B. Members of Congress have asked for an investigation into whether JBS used funds obtained through bribes to purchase Swift & Co and Pilgrim Pride, giving them a stronghold on the industry. In a separate action, JBS agreed to pay fines to settle charges related to a national pork price fixing scheme. Farmers received $28B in assistance to offset losses related to the pandemic. JBS was the recipient of $62.5M in relief. The Batista brothers, owners of JBS, are each worth $3.4B. JBS USA Holdings, a subsidiary of JBS S.A., Brazilian parent company, has annual sales over $50B.

JBS paid $11M to Russian cybercriminals, REvil, to resolve a ransomware attack this month. The House Oversight and Reform Committee has asked JBS to turn over all documents related to the ransomware attack and records of its communications with REvil.

The FBI provides the following regarding how to respond to a ransomware attack:

> The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity.

Teamsters Refuse to Pay Ransom

The Teamsters were hit with a ransomware attack in 2019 but refused to pay the $2.9M ransom to restore access to its electronic files. Union officers were divided over whether to pay the ransom and even bargained the ransom down to $1.1M.

However, only one of two email systems was frozen. They decided not to pay and used archived materials to rebuild their systems, effectively rebuilding 99% of the data, without repercussions.

The FBI recommends keeping operating systems, software, and applications up to date; run regular security scans; backup data regularly; secure backups (make sure they are not connected to the computers and networks they are backing up.

EVOTEK Cybersecurity Predictions

Hit or Miss?

EVOTEK leadership, Matt Stamper, CISO, Executive Advisor, and Macy Dennis, CSO, provided 2021 cybersecurity predictions to CSW. Now that we are halfway into the year, let's look at whether industry movement matches expectations.

Matt Stamper - "2021 will be the year of SOAR and investments in enhanced detention technologies including deception. I am cautiously optimistic that the improvements in security automation, the outstanding work in discovering zero-day vulnerabilities, and other software flaws will improve such that we'll see real reductions in dwell time. I also predict that cybersecurity as a topic for the board of directors will continue to be front-and-center – notably for public companies who are required by the SEC to provide accurate and complete disclosures related to their cyber risks. This focus will drive enhancements as to how organizations address patching and vulnerability management for their technology stacks. Sadly, we will also see the loss of life where OT or heathcare-related technologies are compromised, exposing new levels of liability for organizations in critical sectors."

Macy Dennis –

- "Organizations will increase focus on application and cloud security-focused programs. They will enable the remote workforce, Data Protection Programs, CMMC Certifications."
- "Organizations will improve their Incident Response process and conduct more IR Workshops and Tabletops."
- "Organizations will focus on more services around DevOps, CI/CD pipeline vulnerability testing, and vulnerability management systems."
- "Products and solutions will be more cloud/SaaS focused, primarily due to COVID."
- "Clients will be more focused on outsourcing services with minimal products."

- "2021 will see many moving more systems to the cloud and SaaS solutions.
- "Organizations need to assess themselves with a risk-based focus – this will include building out a risk register and performing more threat modelling exercises to identify the organization's overall true risk posture."
- There is not going to be much change in 2021 with the WFH aspect. People feel safe sitting at home. But they are more likely to be a bigger target and easier to access. Those companies that didn't plan to secure their workforce at home better will need to and, if not, will find themselves in a bad spot.
- "I predict the ransomware attacks to climb as the nation-states are using it to fund their operations. And because of this, the security budgets will increase.
- "2021 will also see Organizations focus more on a Zero Trust model."

Zero Trust rules are enforced on the Cloudflare edge
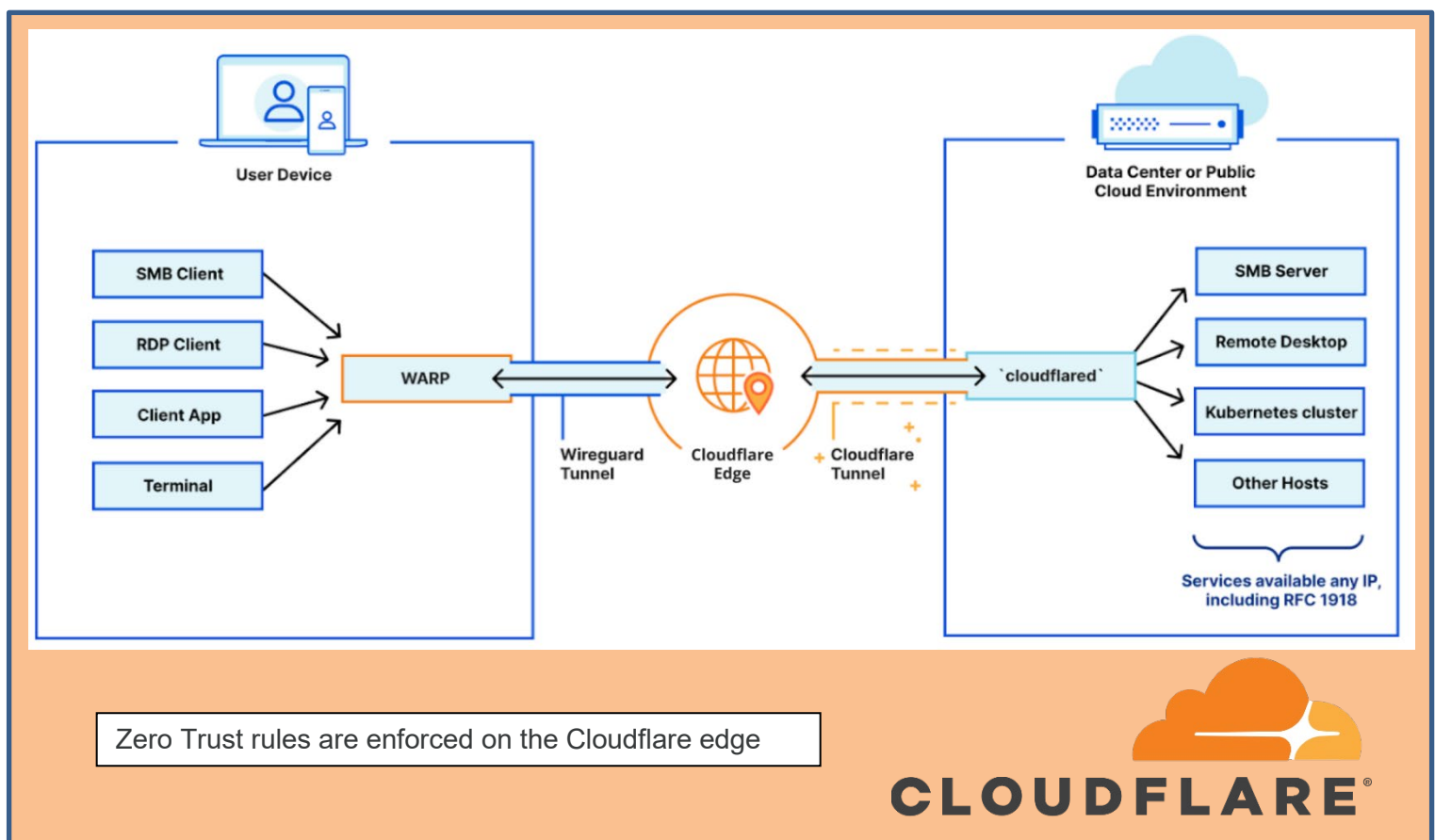
A Zero Trust solution requires operational capabilities that: 1) Never trust, always verify, 2) Assume breach - continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity, 3) Verify explicitly – Access to all resources should be conducted in a consistent and secure manner using multiple attributes (dynamic and static) to derive confidence levels for contextual access decisions to resources. Top Zero Trust vendors include Akamai, Cisco, Cloudflare, Illumio, Palo Alto Networks, Symantec/Broadcom, Okta, and Forcepoint.

AI & Machine Learning in Neurology

AI and Machine Learning Use Cases and Applications in Neurology range from diagnosis to treatment to adapting neural connections and response for movement after spinal cord injuries resulting in paralysis.

Oncology

- Machine learning algorithm using MRI scans of patients with brain tumors to detect and localize tumors for use in diagnoses and tracking therapy response.
- Support vector machine using MRI-based blood volume distribution data to predict preoperative glioma survival

A challenge during brain surgeries is biopsy turnaround time can be as long as 30 minutes, while the patient is anesthetized and not otherwise receiving treatment. Invenio Imaging provides stimulated Raman Histology to image unprocessed tissue specimen without sectioning or staining. It has been successfully used in 1500 brain tumor procedures and reduces diagnostic wait times to less than 3 minutes. The Stimulated Ramon Scattering (SRS) microscope rapidly generates microscopic images of fresh human tissue in the operating room, avoiding the need to unnecessarily remove healthy tissue for analysis and maximizing detection of tumors.

This image, acquired interoperatively with the NIO laser Imaging System in under 3 minutes, highlights the biphasic nature of pilocytic astrocytomas. The piloid component of the tumor contains fire hair-like glial projections and corkscrewing Rosenthal fibers. The spongy component is loosely organized and largely acellular. From case reviews, Invenio Imaging.
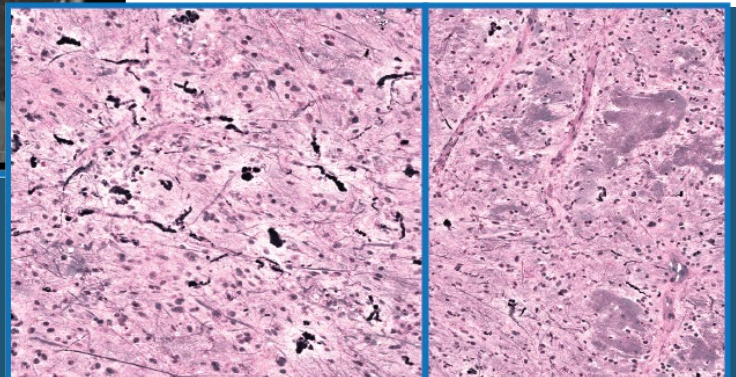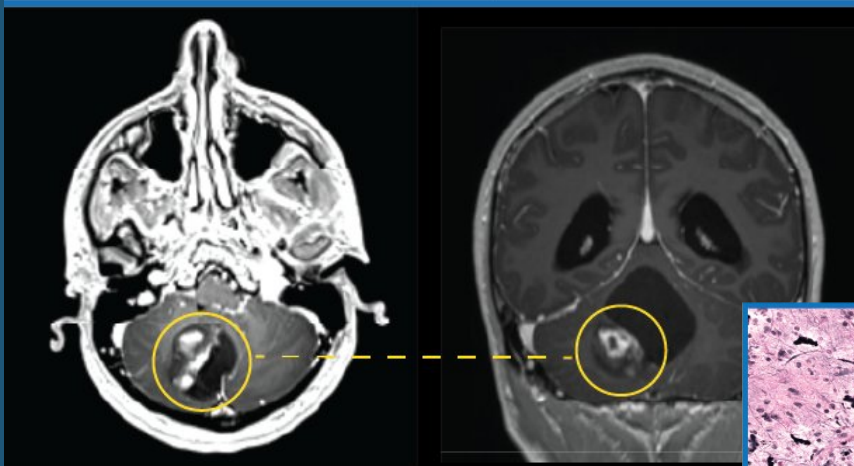
Neurodegeneration

- Application of [AI kinematic data](#) for diagnosis and assessment of Parkinson's disease
- AI has been applied to speech recordings, cognitive test scores, and neuroimaging to measure biomarkers of Alzheimer's disease, including [rate of brain atrophy](#)
- A team from [IBM](#) and [Pfizer](#) has trained AI models to spot [early signs of Alzheimer's disease by analyzing writing](#), looking at linguistic patterns in word usage
- Researchers singled out five RNA-binding proteins previously unlinked to ALS
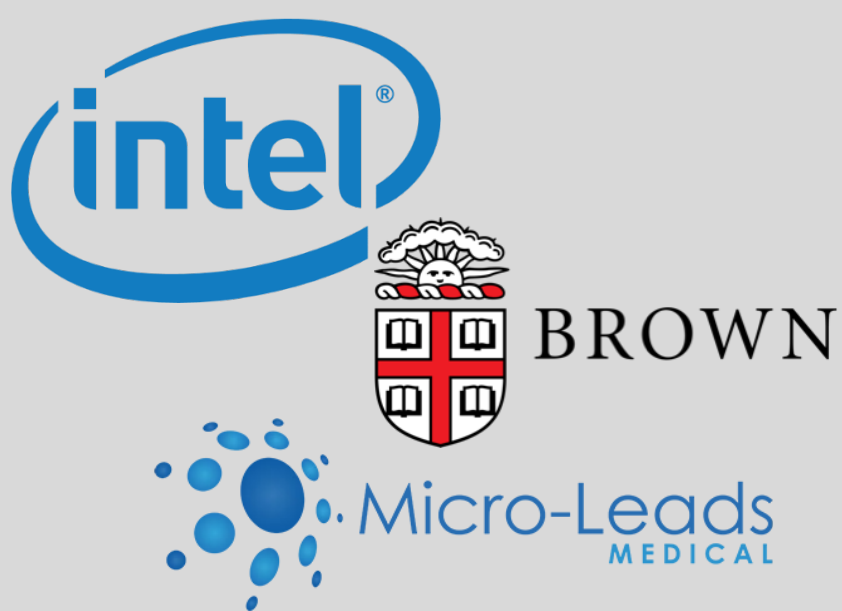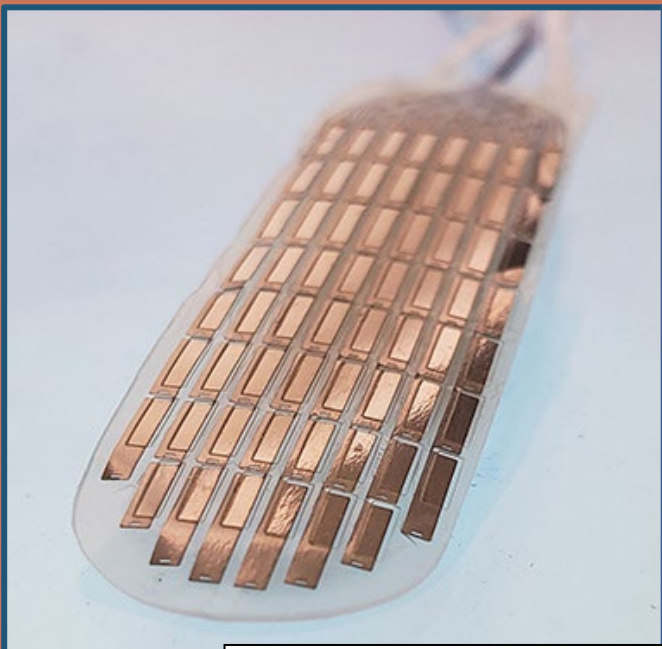
Neurovascular

- Multiple applications in the [diagnosis of strokes](#)
- [Real-time monitoring](#) for patients to adhere to medication schedules and monitor behavior to improve therapeutic outcomes

Traumatic Brain Injury

- ML use in predicting [30-day mortality](#) for traumatic brain injury patients
- AI to determine [severity and type](#) of brain injury

Spinal Cord Injury

- Algorithm [decodes the neuronal activity and control activation of forearm muscles](#) through a custom-built electrical stimulation system to enable use of hands and arms
- [Intel](#) and [Brown University](#) are working on [DARPA-backed intelligent Spine Interface project](#) using AI to restore movement and bladder control. The project will make use of a high-resolution spinal cord stimulation technology developed by [Micro-Leads](#), called [HD64](#).

[Electrode arrays like this one](#) will be used to create an Intelligent Spine Interface aimed at one day helping restore function for people with spinal cord injuries.

How to Take a 360 Degree View of Cybersecurity

with Security Scorecard and Crowe

To what extent does your organization have a 3rd party risk assessment plan/practice (check one; answers anonymous):

We continuously assess 3rd party risk:	20%
We assess 3rd party risk on a periodic (annual or better) basis:	20%
We assess 3rd party risk when bringing on all new vendors:	0%
We have assessed 3rd party risks after security incidents:	0%
We are exploring implementing a 3rd party risk program:	20%
We are too small to consider 3rd party risk:	0%
Don't know:	40%

How to Take a 360 Degree View of Cybersecurity

How "close" have you been to a 3rd party-based breach (check one; answers are anonymous):

Our company has had a confirmed 3rd party-based breach:	66%
We have had a 3rd party vendor that suffered a breach:	0%
We have used products that were breached:	0%
We don't know whether we have had a 3rd party breach:	0%
We can confidently say we have not had a 3rd party breach:	33%

G2M Research Multi-Vendor Webinar Series

Our webinar, Tuesday, June 15 "It's 2021 - Where Has NVMe-oF™ Progressed To?" with sponsors Lightbits Labs and KIOXIA:

> NVMe-oF will be seven years old as of September 2021. Most storage companies, analysts, and NVMexpress.org (the parent organization for NVMe and NVMe-oF) say that NVMe-oF is "the future", yet the number of production implementations is fairly small. Where is NVMe-oF today, and what does its future looks like?

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.

July 13:	Computational Storage vs Virtualized Computation/Storage in the Datacenter: "And The Winner Is"?
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

June 21-23	VIRTUAL VOICE
June 22	Think Cybersecurity for Government 2021
June 22-23	Virtual Cybersecurity Summit: Canada
June 22-25	ITEXPO 2021
June 23	Governance, Risk, & Compliance ConfEx
June 23	Virtual Seattle/Portland Cybersecurity Summit 2021
June 29	Virtual Philadelphia Cybersecurity Summit 2021
June 29-30	Geekle Cybersecurity Global Summit 2021
June 30	FutureCon Chicago
July 7	Virtual St. Louis/OKC Cyber Security Summit
July 7	FutureCon Seattle
July 12-15	DFRWS USA
July 13-14	ISMG Virtual Cybersecurity Summit: Government
July 14	The Future of AI
July 14-18	Industrial Conference on Data Mining (ICDM)
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

Effective Marketing & Communications
with Quantifiable Results