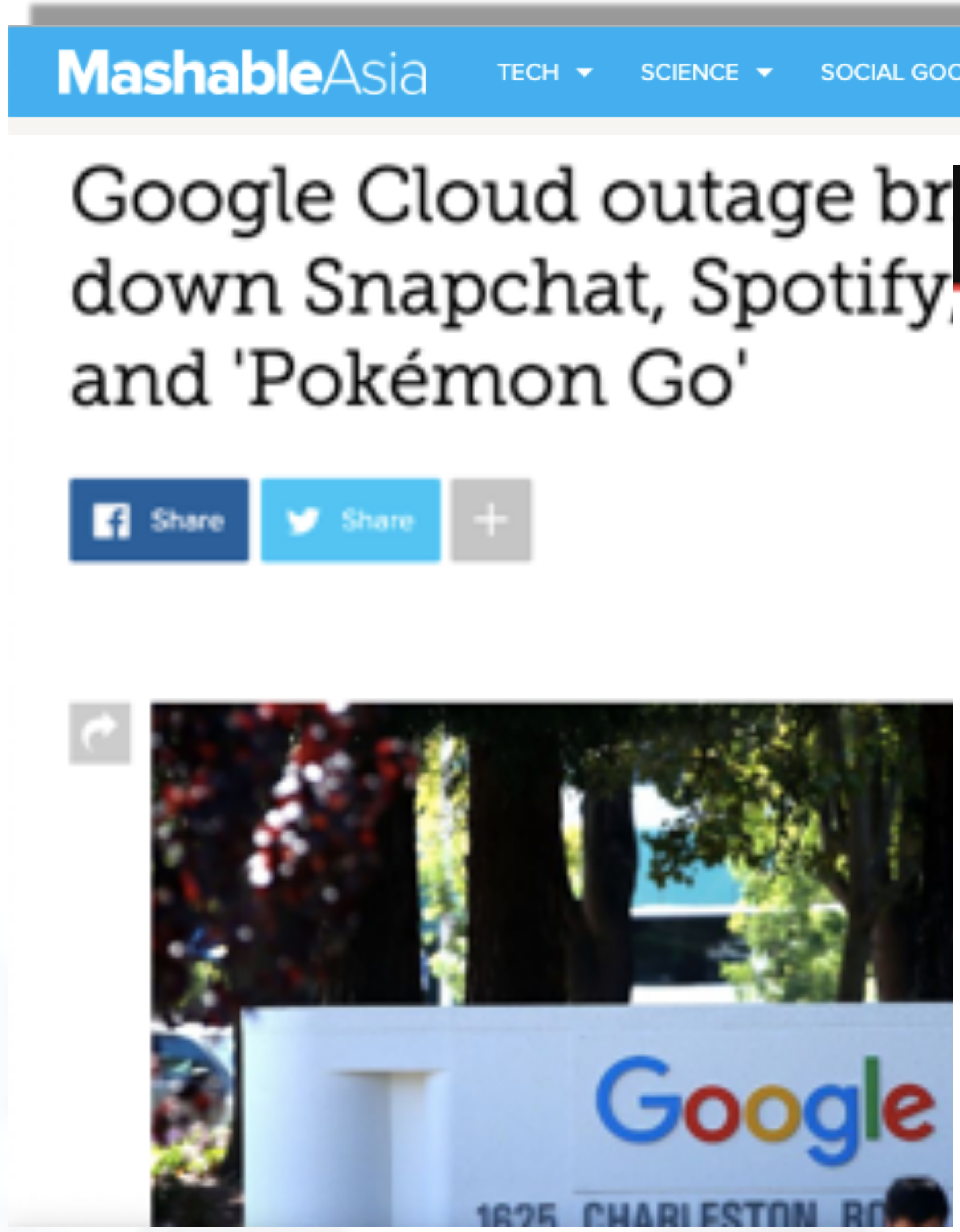
CLOUD INCIDENTS – ARE YOU PREPARED?

LOW Chee Hao
Cyber Security Consultant
LGMS Sdn Bhd

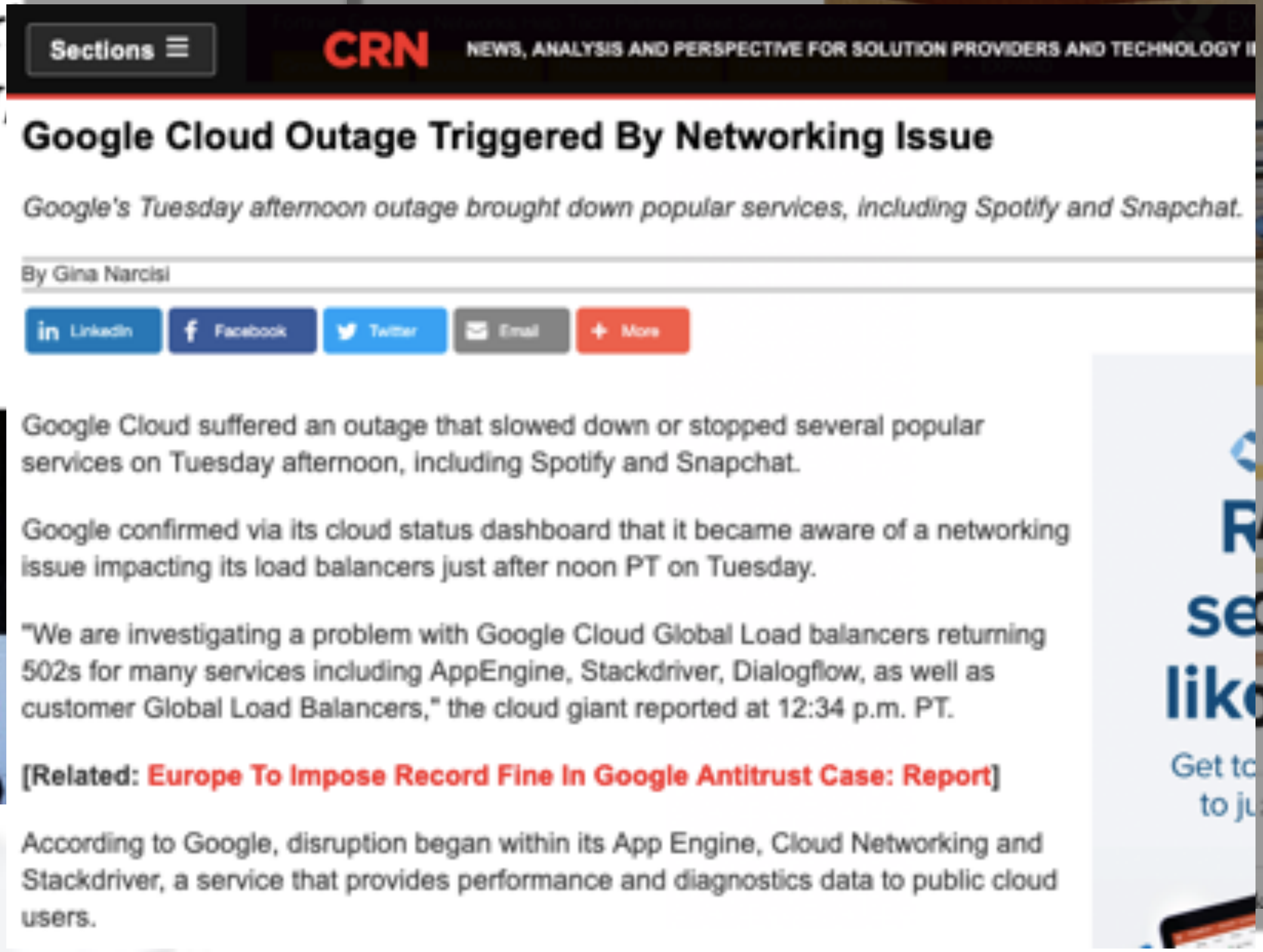
CSA cloud security alliance®

Recent Cloud Incidents (Outage)

Google Cloud Platform



Google Cloud outage br
down Snapchat, Spotify
and 'Pokémon Go'



Sections
CRN
NEWS, ANALYSIS AND PERSPECTIVE FOR SOLUTION PROVIDERS AND TECHNOLOGY I
LinkedIn
Facebook
Twitter
Email
More

Google Cloud Outage Triggered By Networking Issue

Google's Tuesday afternoon outage brought down popular services, including Spotify and Snapchat.

By Gina Narcisi

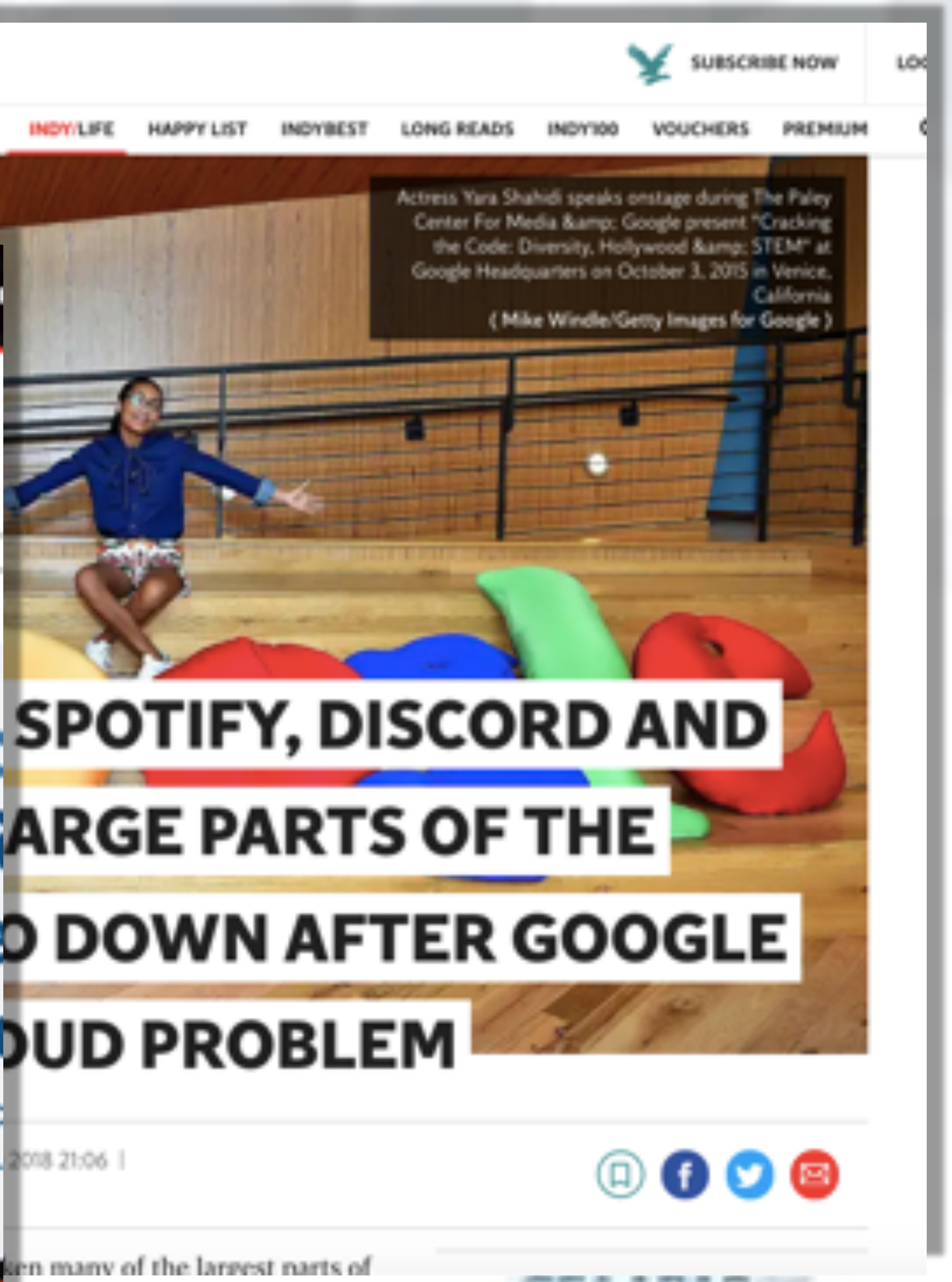
Google Cloud suffered an outage that slowed down or stopped several popular services on Tuesday afternoon, including Spotify and Snapchat.

Google confirmed via its cloud status dashboard that it became aware of a networking issue impacting its load balancers just after noon PT on Tuesday.

"We are investigating a problem with Google Cloud Global Load balancers returning 502s for many services including AppEngine, Stackdriver, Dialogflow, as well as customer Global Load Balancers," the cloud giant reported at 12:34 p.m. PT.

[Related: Europe To Impose Record Fine In Google Antitrust Case: Report]

According to Google, disruption began within its App Engine, Cloud Networking and Stackdriver, a service that provides performance and diagnostics data to public cloud users.



Actress Yara Shahidi speaks onstage during The Paley Center For Media &amp; Google present "Cracking the Code: Diversity, Hollywood &amp; STEM" at Google Headquarters on October 3, 2015 in Venice, California (Mike Windle/Getty Images for Google)

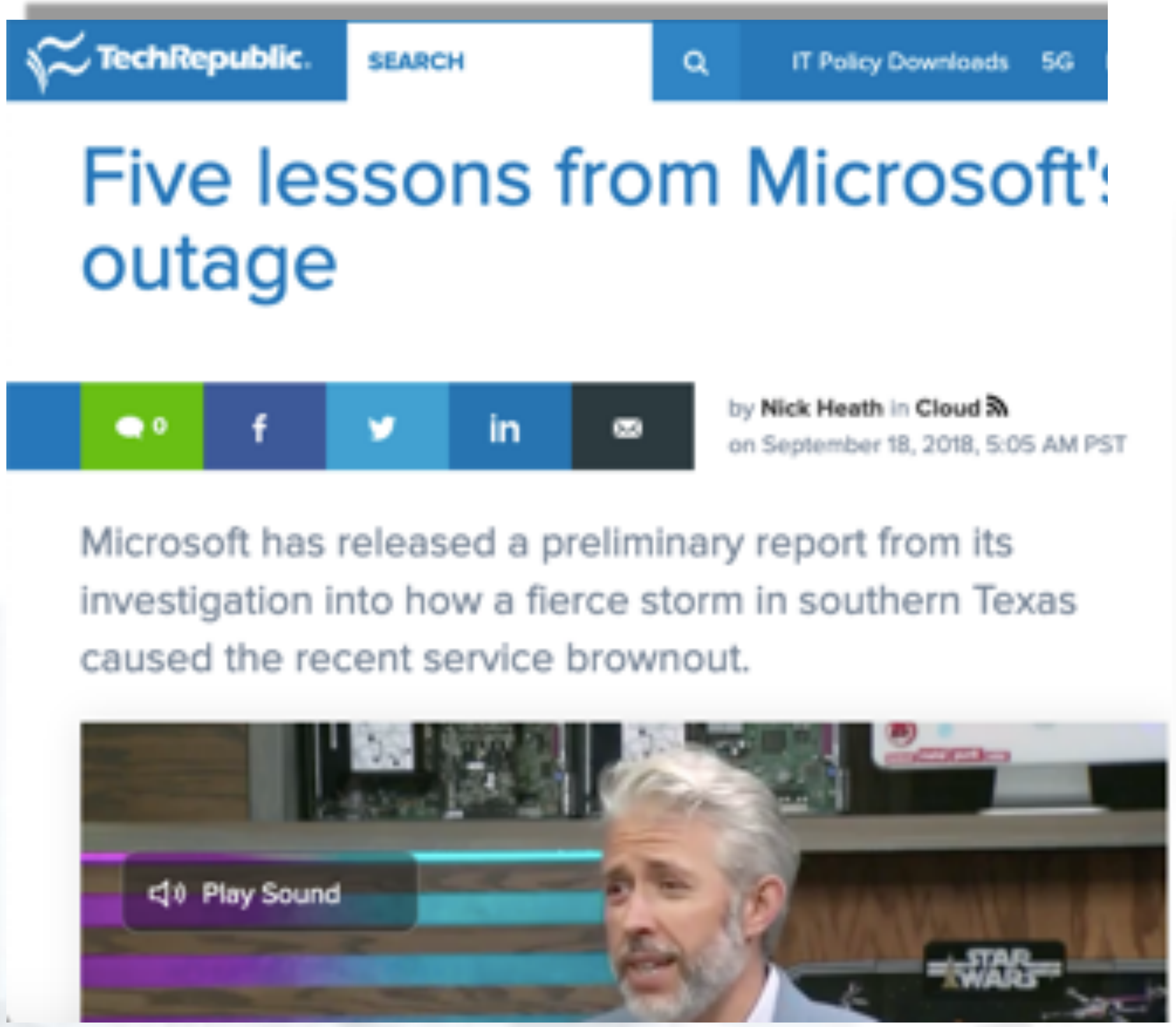
SPOTIFY, DISCORD AND
ARGE PARTS OF THE
D DOWN AFTER GOOGLE
OUD PROBLEM

2018 21:06

en many of the largest parts of

Recent Cloud Incidents (Outage)

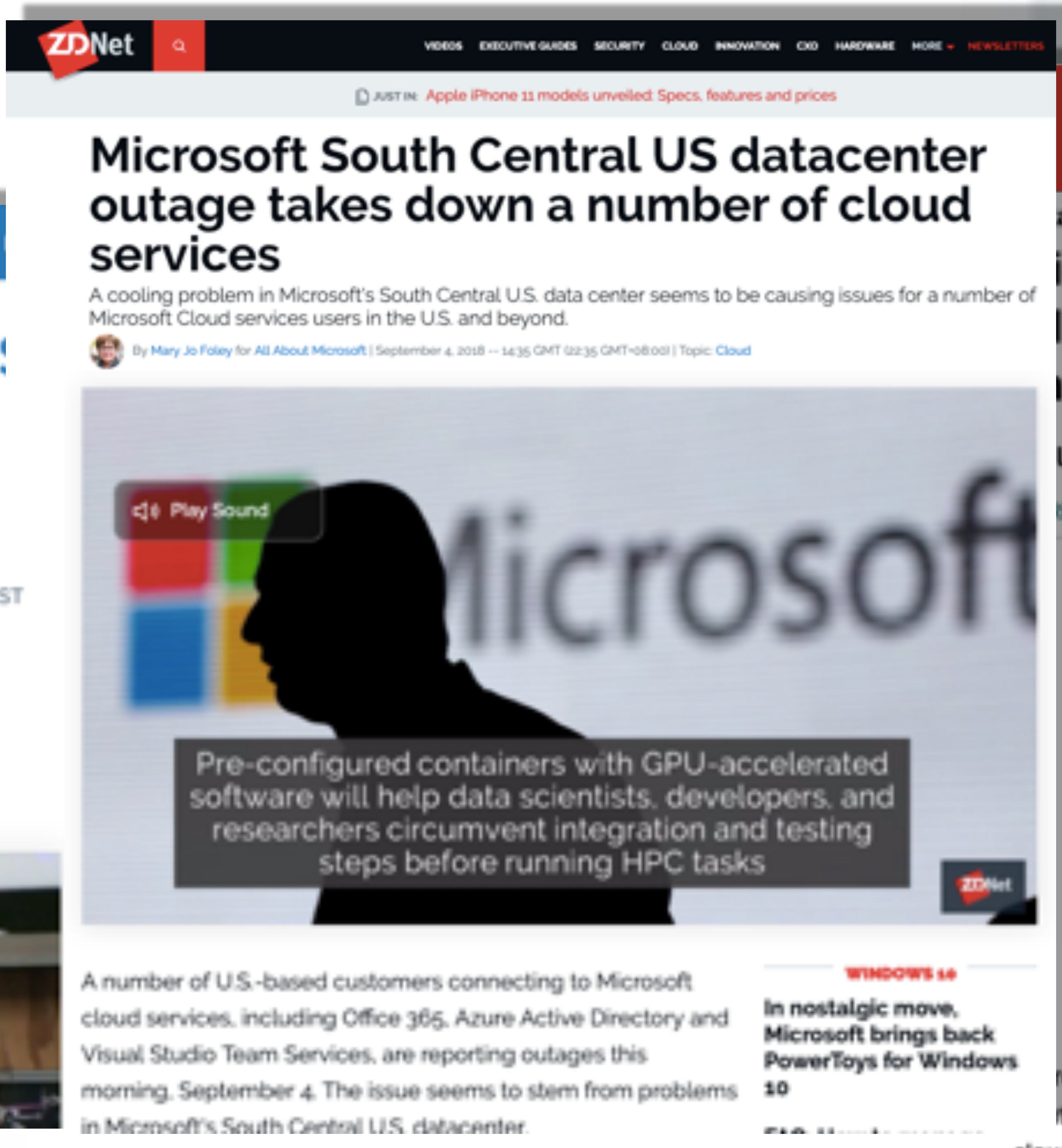
Microsoft Azure



Five lessons from Microsoft's outage

by Nick Heath in Cloud
on September 18, 2018, 5:05 AM PST

Microsoft has released a preliminary report from its investigation into how a fierce storm in southern Texas caused the recent service brownout.



Microsoft South Central US datacenter outage takes down a number of cloud services

A cooling problem in Microsoft's South Central U.S. data center seems to be causing issues for a number of Microsoft Cloud services users in the U.S. and beyond.

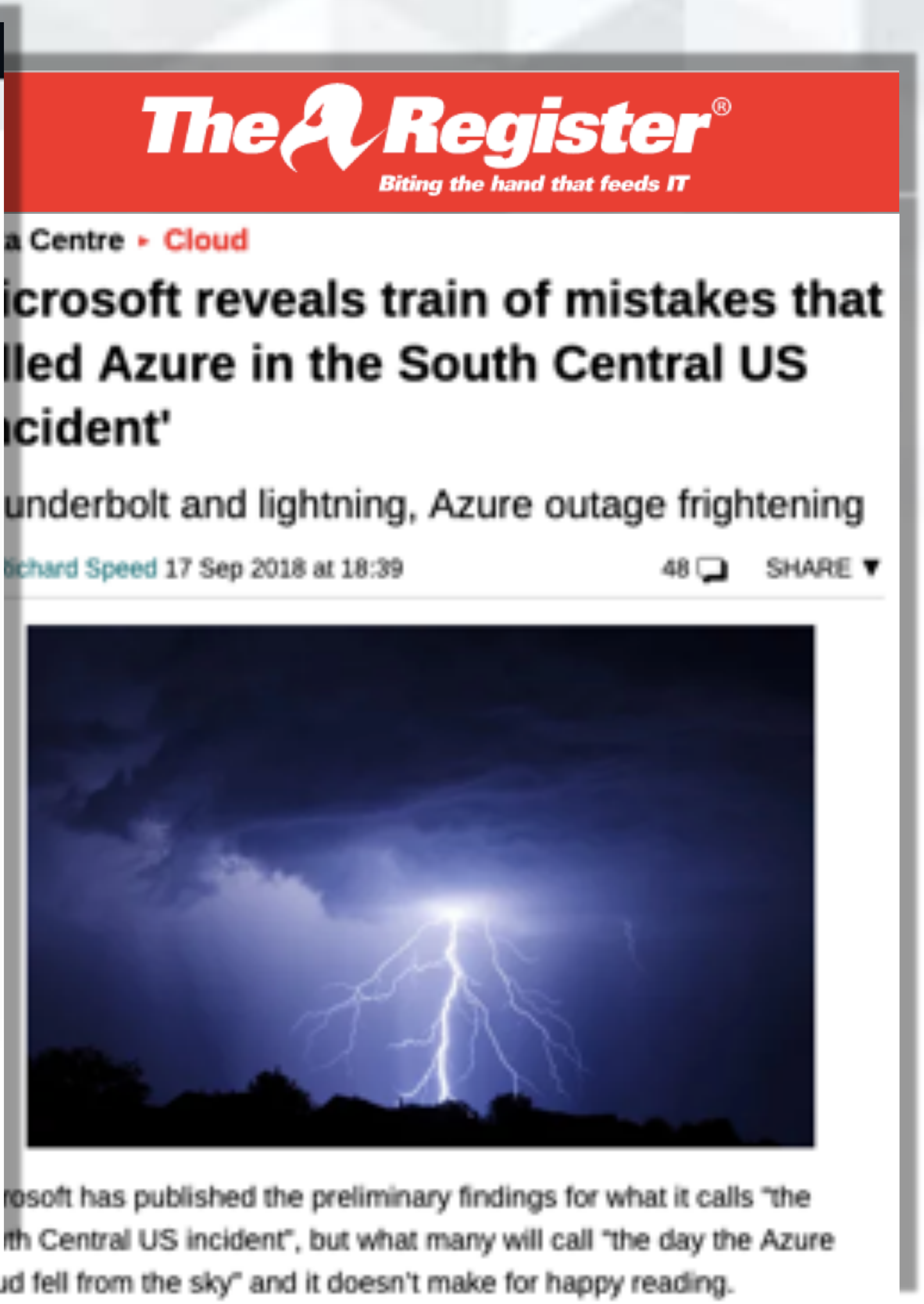
By Mary Jo Foley for All About Microsoft | September 4, 2018 -- 14:35 GMT (22:35 GMT+08:00) | Topic: Cloud

Pre-configured containers with GPU-accelerated software will help data scientists, developers, and researchers circumvent integration and testing steps before running HPC tasks

A number of U.S.-based customers connecting to Microsoft cloud services, including Office 365, Azure Active Directory and Visual Studio Team Services, are reporting outages this morning, September 4. The issue seems to stem from problems in Microsoft's South Central U.S. datacenter.

WINDOWS 10

In nostalgic move, Microsoft brings back PowerToys for Windows 10



a Centre ▸ Cloud

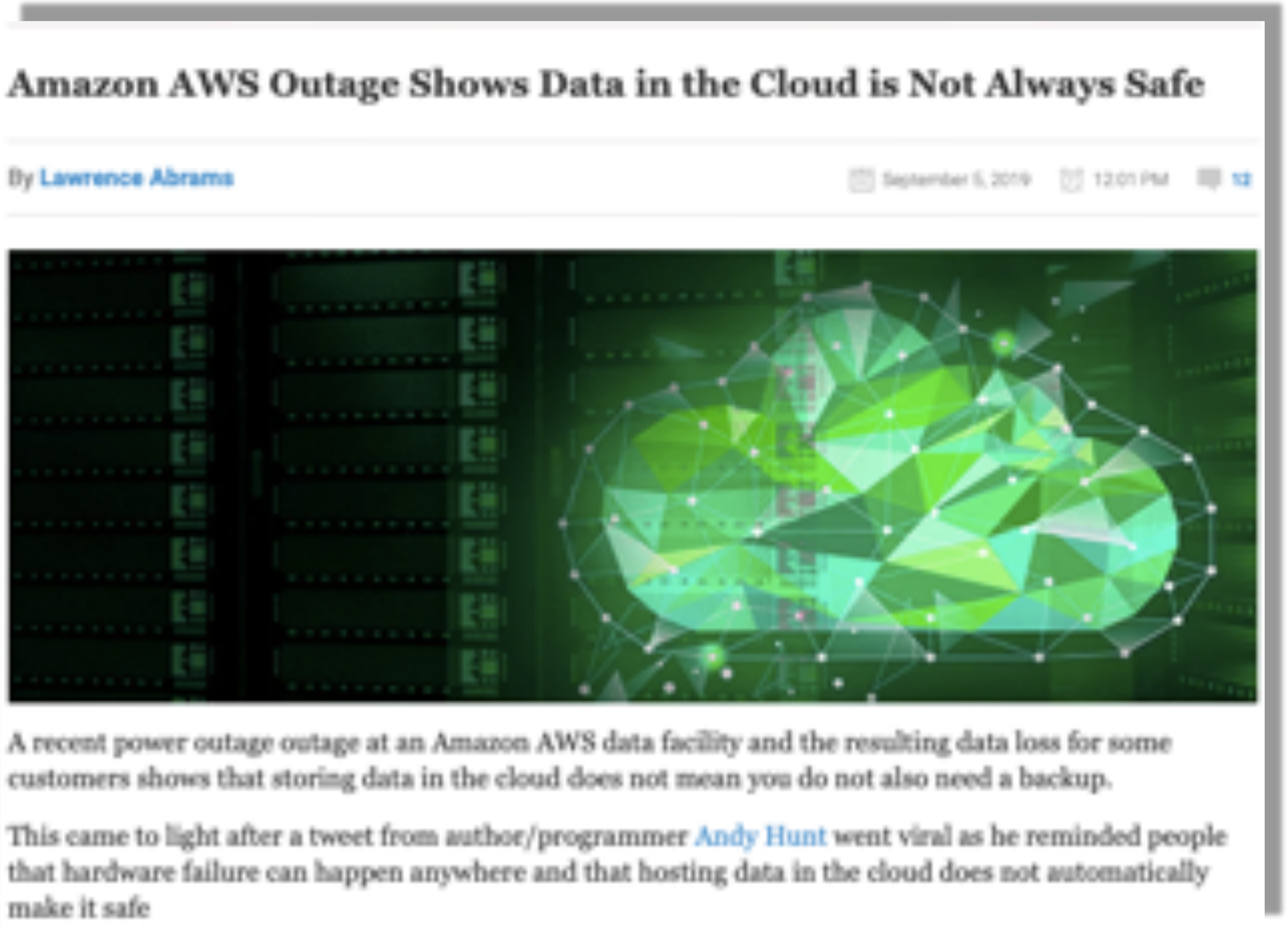
icrosoft reveals train of mistakes that lled Azure in the South Central US cident'

underbolt and lightning, Azure outage frightening

chard Speed 17 Sep 2018 at 18:39 48 SHARE ▼

rosoft has published the preliminary findings for what it calls "the th Central US incident", but what many will call "the day the Azure cloud fell from the sky" and it doesn't make for happy reading.

Recent Cloud Incidents (Outage)

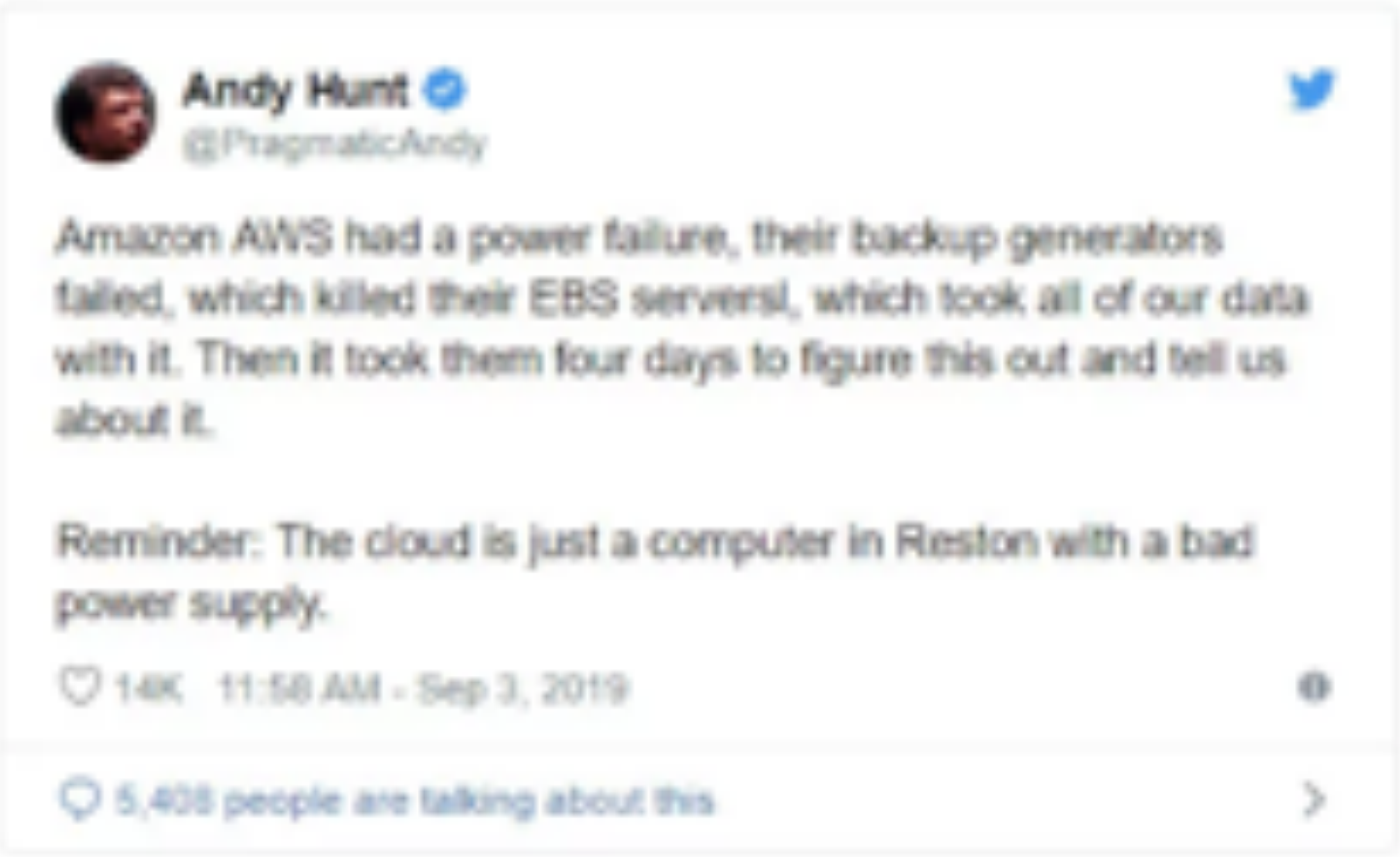


Amazon AWS Outage Shows Data in the Cloud is Not Always Safe

By Lawrence Abrams September 5, 2019 12:01 PM 12

A recent power outage outage at an Amazon AWS data facility and the resulting data loss for some customers shows that storing data in the cloud does not mean you do not also need a backup.

This came to light after a tweet from author/programmer Andy Hunt went viral as he reminded people that hardware failure can happen anywhere and that hosting data in the cloud does not automatically make it safe



Andy Hunt
@PragmaticAndy

Amazon AWS had a power failure, their backup generators failed, which killed their EBS servers!, which took all of our data with it. Then it took them four days to figure this out and tell us about it.

Reminder: The cloud is just a computer in Reston with a bad power supply.

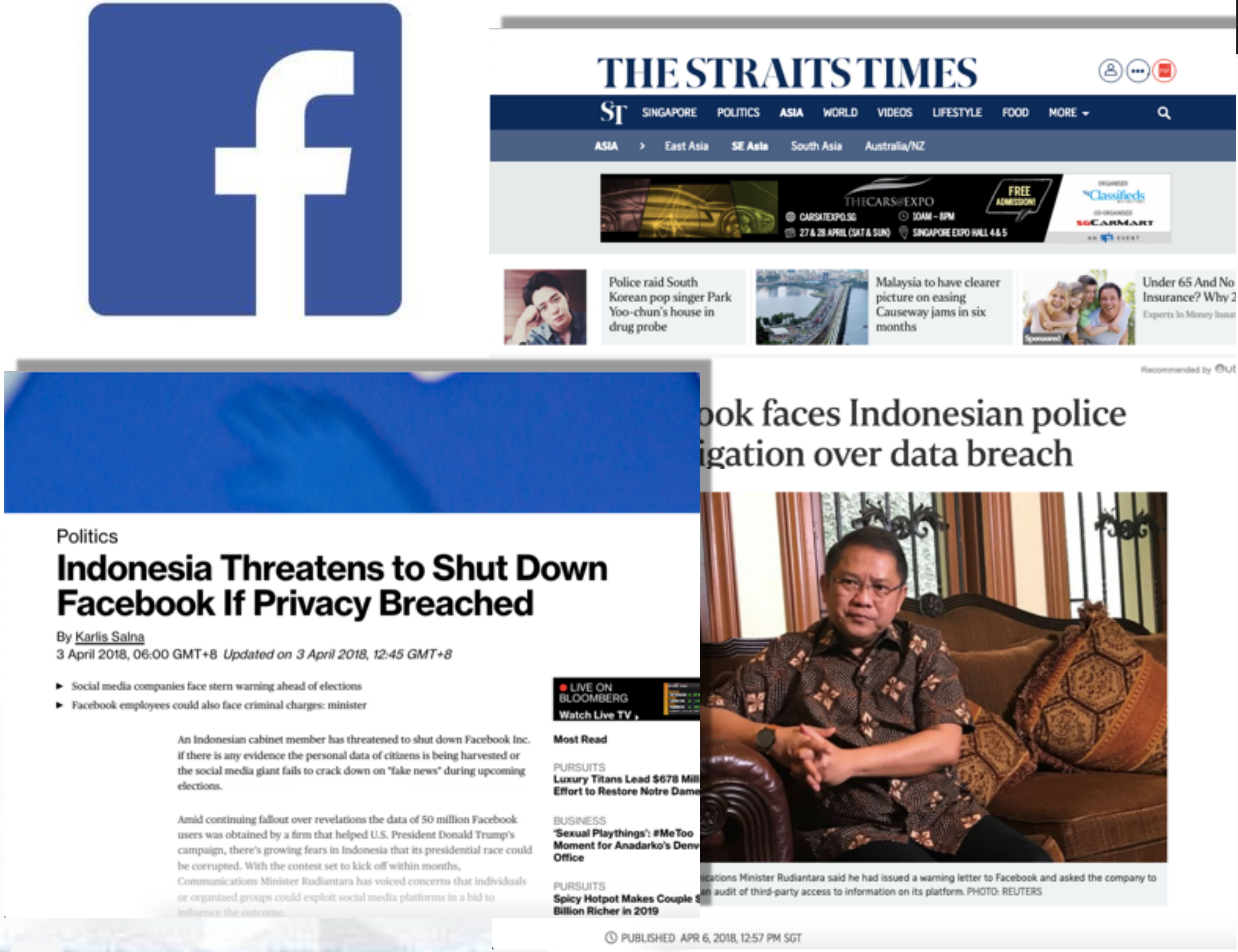
♡ 14K 11:58 AM - Sep 3, 2019

5,408 people are talking about this

Hunt's data were eventually NOT recovered..

AWS:
"Due to the damage from the power event, the EBS servers underlying these volumes have not recovered. After further attempts to recover these volumes, they were determined to be unrecoverable."

Major Cloud Incidents (Data Breach)



THE STRAITS TIMES

ST SINGAPORE POLITICS ASIA WORLD VIDEOS LIFESTYLE FOOD MORE

ASIA › East Asia SE Asia South Asia Australia/NZ

Police raid South Korean pop singer Park Yoo-chun's house in drug probe

Malaysia to have clearer picture on easing Causeway jams in six months

Under 65 And No Insurance? Why 2

Experts In Money Insur

Sponsored

Recommended by Out

ook faces Indonesian police igation over data breach

ications Minister Rudiantara said he had issued a warning letter to Facebook and asked the company to an audit of third-party access to information on its platform. PHOTO: REUTERS

PUBLISHED APR 6, 2018, 12:57 PM SGT

Politics

Indonesia Threatens to Shut Down Facebook If Privacy Breached

By Karlis Salna

3 April 2018, 06:00 GMT+8 *Updated on 3 April 2018, 12:45 GMT+8*

- Social media companies face stern warning ahead of elections
- Facebook employees could also face criminal charges: minister

An Indonesian cabinet member has threatened to shut down Facebook Inc. if there is any evidence the personal data of citizens is being harvested or the social media giant fails to crack down on "fake news" during upcoming elections.

Amid continuing fallout over revelations the data of 50 million Facebook users was obtained by a firm that helped U.S. President Donald Trump's campaign, there's growing fears in Indonesia that its presidential race could be corrupted. With the contest set to kick off within months, Communications Minister Rudiantara has voiced concerns that individuals or organized groups could exploit social media platforms in a bid to influence the outcome.

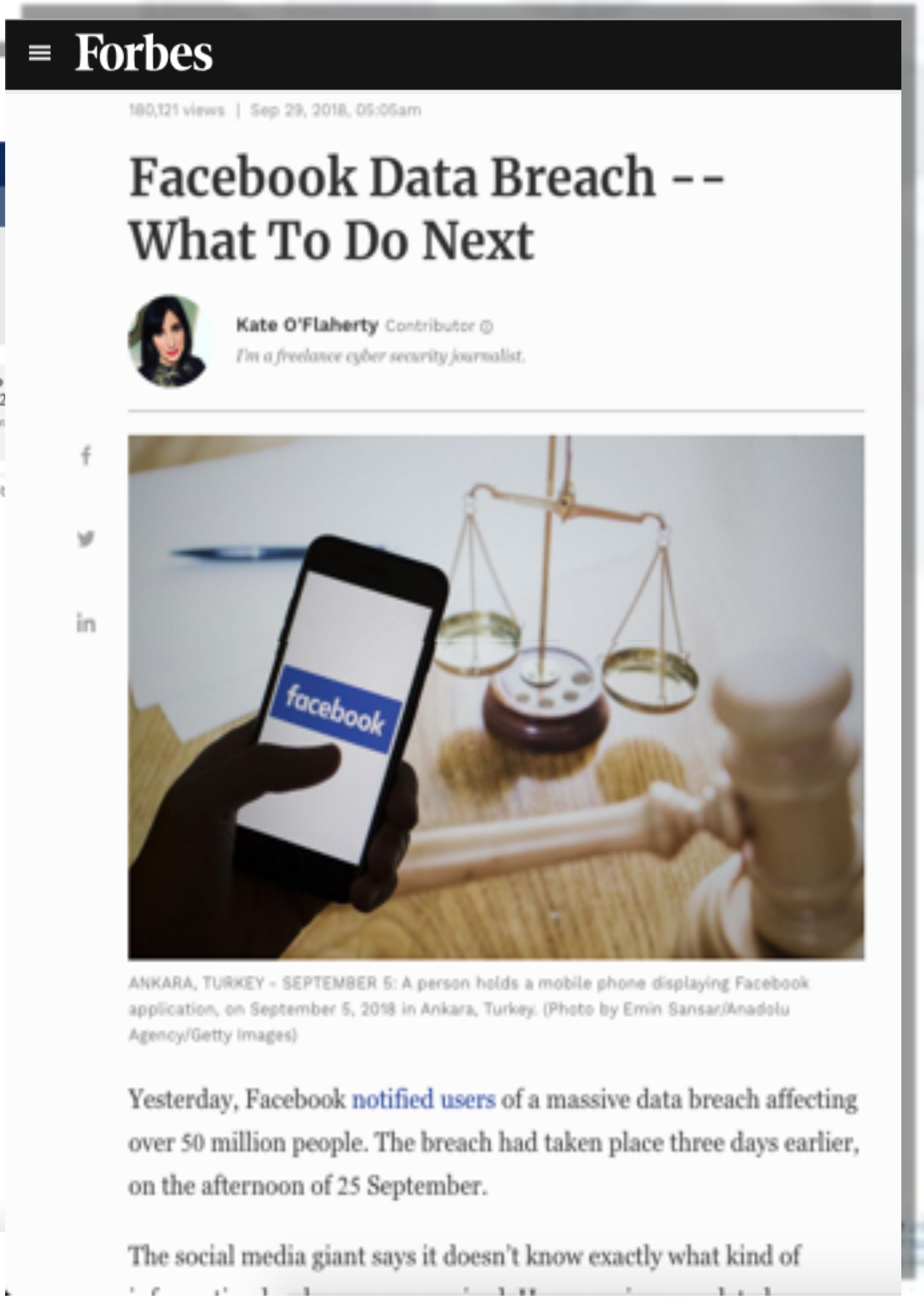
LIVE ON BLOOMBERG Watch Live TV ›

Most Read

PURSUITS
Luxury Titans Lead $678 Mill Effort to Restore Notre Dame

BUSINESS
'Sexual Playthings': #MeToo Moment for Anadarko's Denv Office

PURSUITS
Spicy Hotpot Makes Couple $ Billion Richer in 2019



Forbes

180,121 views | Sep 29, 2018, 05:06am

Facebook Data Breach -- What To Do Next

Kate O'Flaherty Contributor

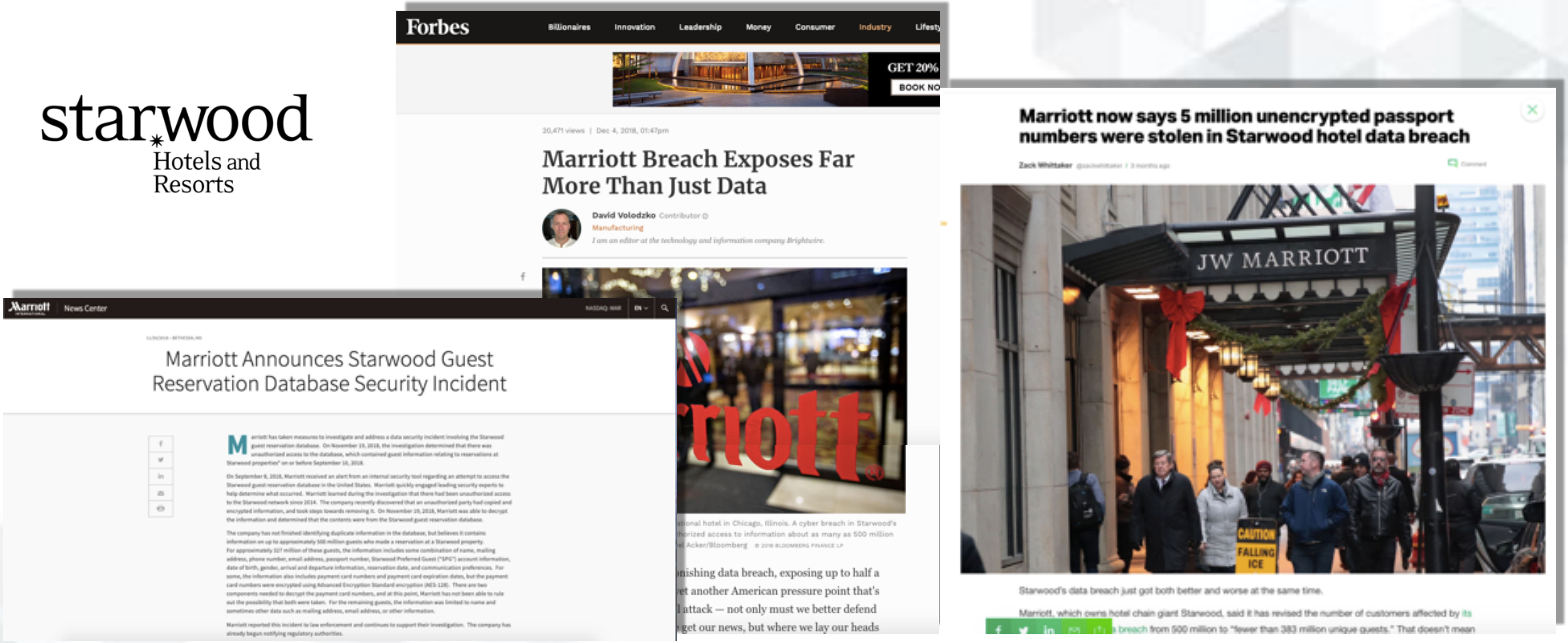
I'm a freelance cyber security journalist.

ANKARA, TURKEY - SEPTEMBER 5: A person holds a mobile phone displaying Facebook application, on September 5, 2018 in Ankara, Turkey. (Photo by Emin Sansar/Anadolu Agency/Getty Images)

Yesterday, Facebook notified users of a massive data breach affecting over 50 million people. The breach had taken place three days earlier, on the afternoon of 25 September.

The social media giant says it doesn't know exactly what kind of

Major Cloud Incidents (Data Breach)



starwood
Hotels and
Resorts

20,471 views | Dec 4, 2018, 01:47pm

Marriott Breach Exposes Far More Than Just Data

David Volodzko Contributor
Manufacturing
I am an editor at the technology and information company Brightwire.

ational hotel in Chicago, Illinois. A cyber breach in Starwood's thorized access to information about as many as 500 million el Acker/Bloomberg © 2018 BLOOMBERG FINANCE LP

nishing data breach, exposing up to half a yet another American pressure point that's l attack — not only must we better defend get our news, but where we lay our heads

11/30/2018 – BETHESDA, MD

Marriott Announces Starwood Guest Reservation Database Security Incident

Marriott has taken measures to investigate and address a data security incident involving the Starwood guest reservation database. On November 19, 2018, the investigation determined that there was unauthorized access to the database, which contained guest information relating to reservations at Starwood properties* on or before September 10, 2018.

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. The company recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

The company has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information.

Marriott reported this incident to law enforcement and continues to support their investigation. The company has already begun notifying regulatory authorities.

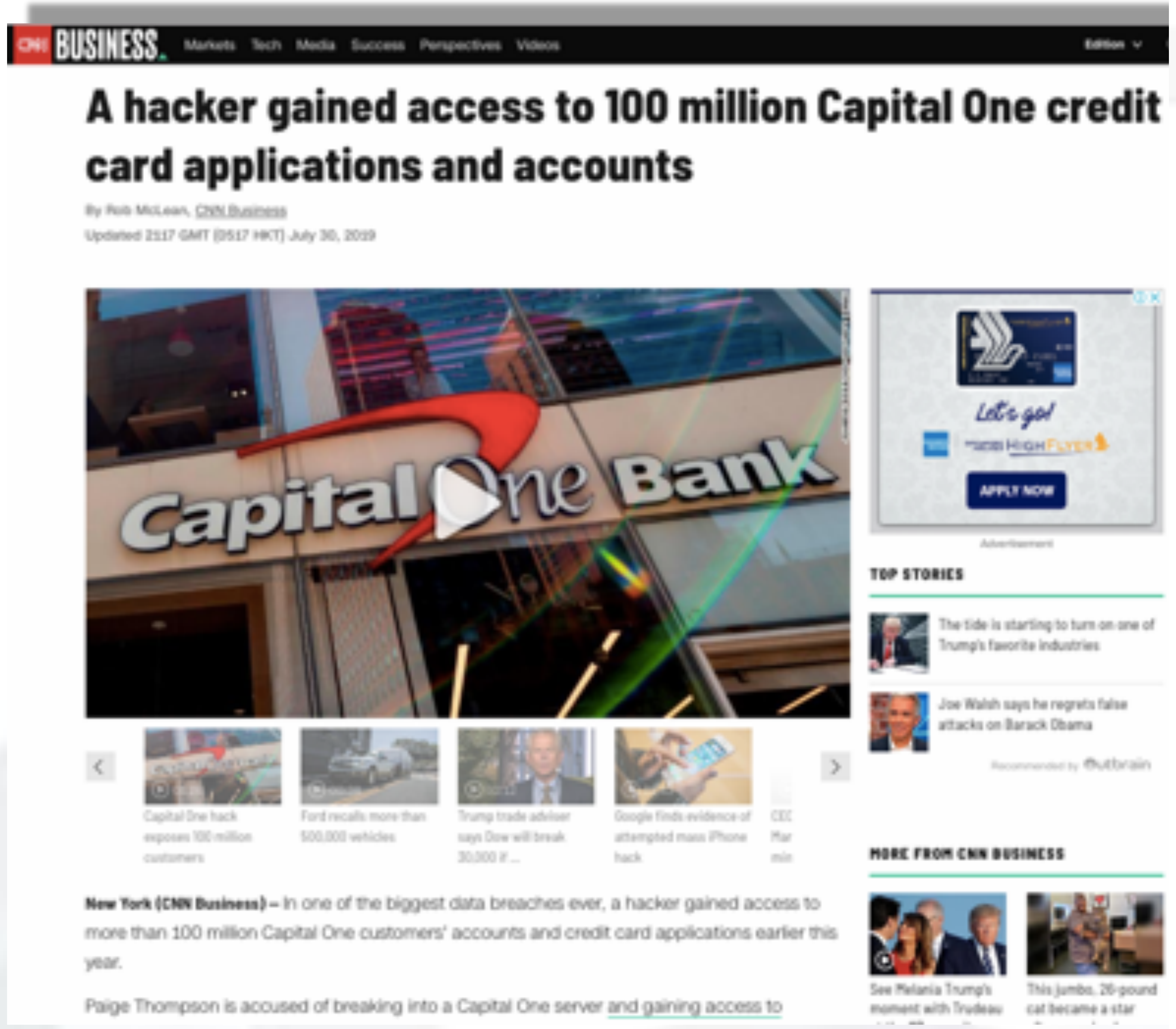
Marriott now says 5 million unencrypted passport numbers were stolen in Starwood hotel data breach

Zack Whittaker @zackwhittaker / 3 months ago Comment

Starwood's data breach just got both better and worse at the same time.

Marriott, which owns hotel chain giant Starwood, said it has revised the number of customers affected by its a breach from 500 million to "fewer than 383 million unique guests." That doesn't mean

Major Cloud Incidents (Data Breach)



CNN BUSINESS
Markets Tech Media Success Perspectives Videos
Edition

A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business

Updated 2117 GMT (0517 HKT) July 30, 2019

Capital One Bank
Capital One hack exposes 100 million customers
Ford recalls more than 500,000 vehicles
Trump trade adviser says Dow will break 30,000 if ...
Google finds evidence of attempted mass iPhone hack

TOP STORIES

The tide is starting to turn on one of Trump's favorite industries

Joe Walsh says he regrets false attacks on Barack Obama

Recommended by Outbrain

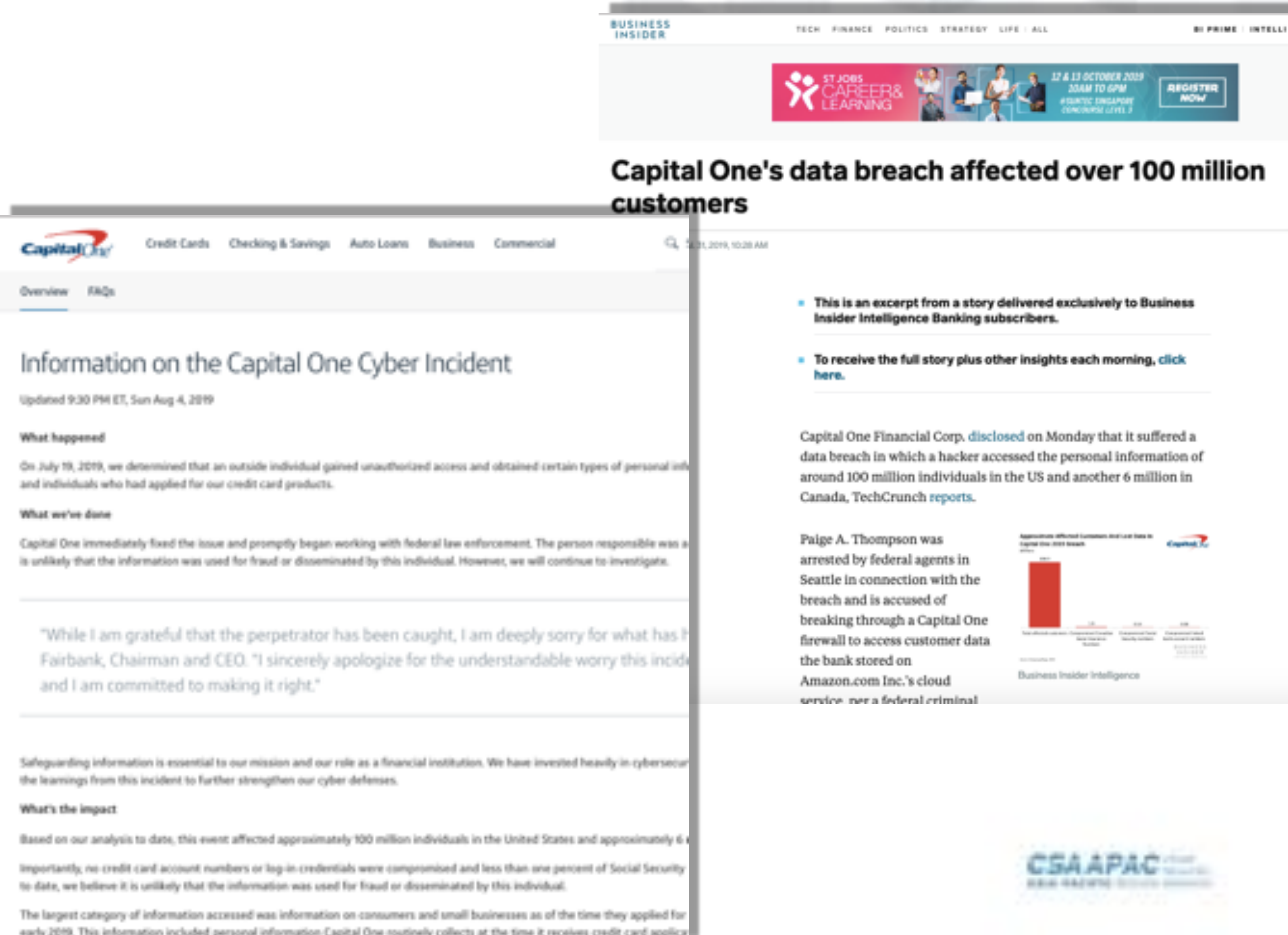
MORE FROM CNN BUSINESS

See Melania Trump's moment with Trudeau

This jumbo, 26-pound cat became a star

New York (CNN Business) – In one of the biggest data breaches ever, a hacker gained access to more than 100 million Capital One customers' accounts and credit card applications earlier this year.

Paige Thompson is accused of breaking into a Capital One server and gaining access to



Capital One
Credit Cards Checking & Savings Auto Loans Business Commercial
Overview FAQs

Information on the Capital One Cyber Incident

Updated 9:30 PM ET, Sun Aug 4, 2019

What happened

On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal inf
and individuals who had applied for our credit card products.

What we've done

Capital One immediately fixed the issue and promptly began working with federal law enforcement. The person responsible was a
is unlikely that the information was used for fraud or disseminated by this individual. However, we will continue to investigate.

> "While I am grateful that the perpetrator has been caught, I am deeply sorry for what has h
> Fairbank, Chairman and CEO. "I sincerely apologize for the understandable worry this incid
> and I am committed to making it right."

Safeguarding information is essential to our mission and our role as a financial institution. We have invested heavily in cybersecur
the learnings from this incident to further strengthen our cyber defenses.

What's the impact

Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6

Importantly, no credit card account numbers or log-in credentials were compromised and less than one percent of Social Security
to date, we believe it is unlikely that the information was used for fraud or disseminated by this individual.

The largest category of information accessed was information on consumers and small businesses as of the time they applied for
early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applica

Capital One's data breach affected over 100 million customers

Jul. 31, 2019, 10:28 AM

- **This is an excerpt from a story delivered exclusively to Business Insider Intelligence Banking subscribers.**
- **To receive the full story plus other insights each morning, click here.**

Capital One Financial Corp. disclosed on Monday that it suffered a data breach in which a hacker accessed the personal information of around 100 million individuals in the US and another 6 million in Canada, TechCrunch reports.

Paige A. Thompson was arrested by federal agents in Seattle in connection with the breach and is accused of breaking through a Capital One firewall to access customer data the bank stored on Amazon.com Inc.'s cloud service, per a federal criminal

Business Insider Intelligence

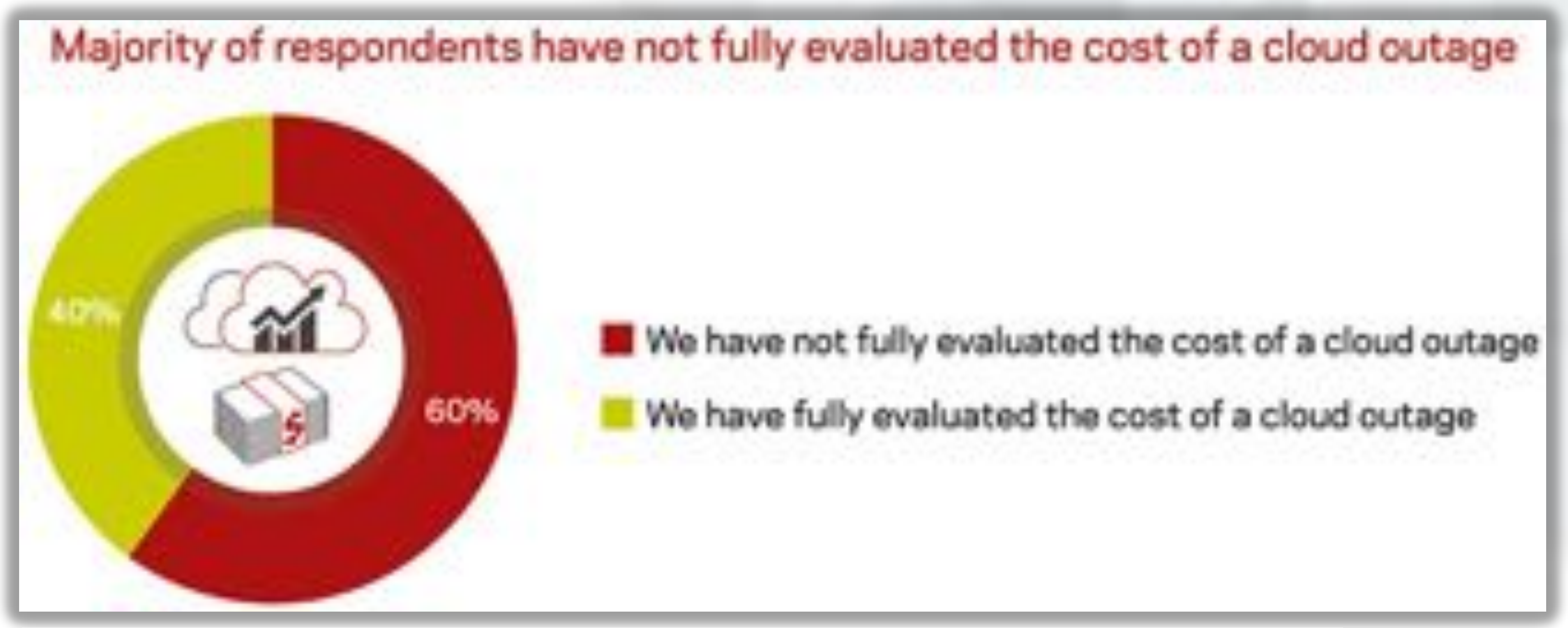
Who Pays for Outages and Incidents?

Cloud Users

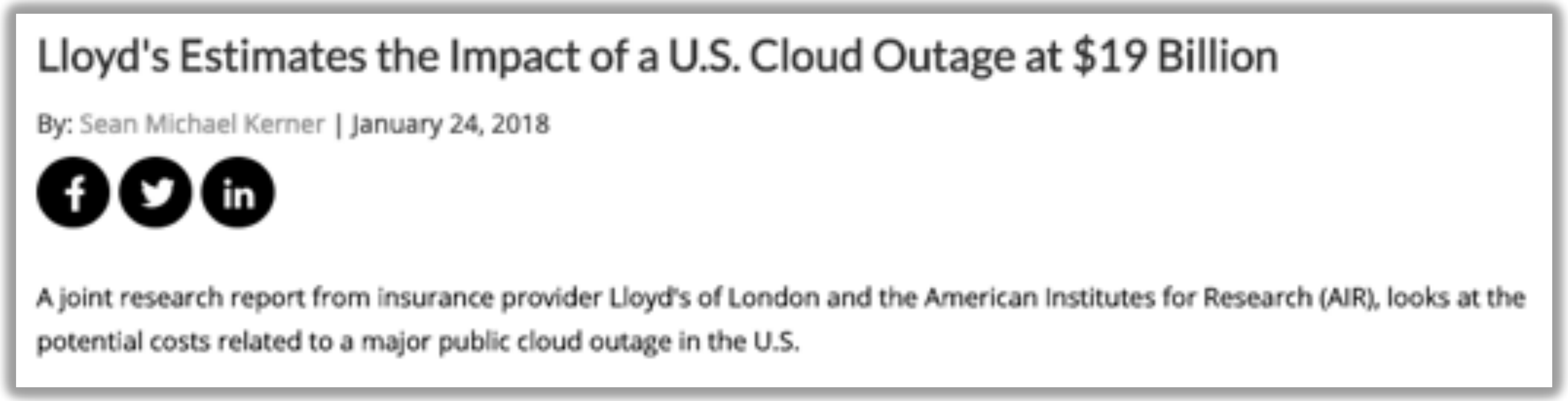
Disruption to businesses (especially SMEs) will undermine confidence in cloud adoption, if not dealt with properly.

Important Pointers:

- Have a stalwart BC plan
- Insure that incidents and outages do not result in a major impact to business
- Prepare for adverse outcome to mitigate risks & respond accordingly



Source: Help Net Security



Lloyd's Estimates the Impact of a U.S. Cloud Outage at $19 Billion

By: Sean Michael Kerner | January 24, 2018

A joint research report from insurance provider Lloyd's of London and the American Institutes for Research (AIR), looks at the potential costs related to a major public cloud outage in the U.S.

Source: eWeek.com

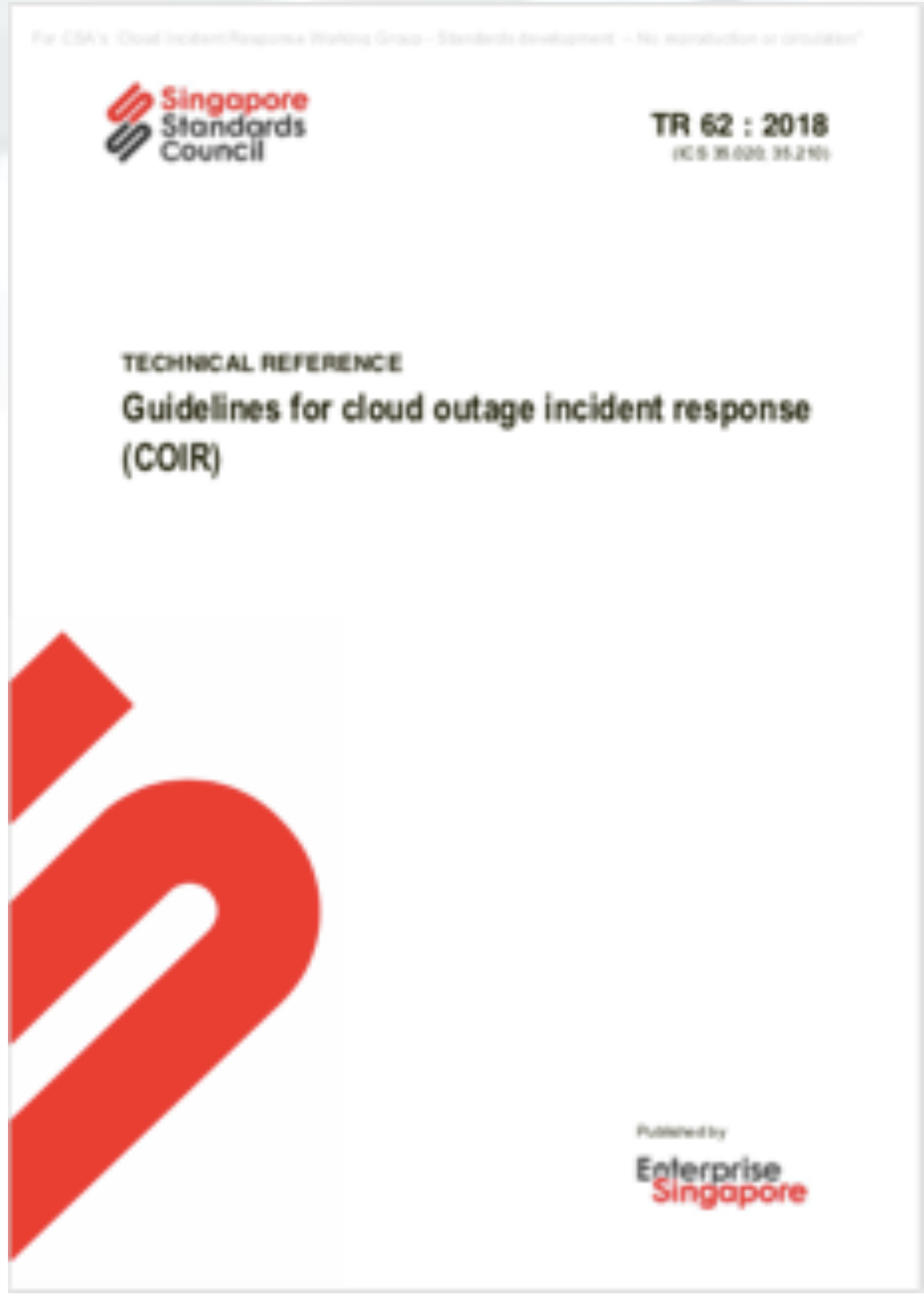
Prior Work – COIR

BACKGROUND

Cloud Outage Incident Response (COIR)

- Different CSPs respond to cloud outages and services levels differently.
- These different approaches require CSCs to spend resources liaising with CSPs for a COIR plan
- Lack of a common COIR framework hinders CSCs in taking preventive measures.

To **mitigate damages and losses** and help **CSCs to choose the appropriate outage protection measures** to complement their own business continuity/IT DR capabilities.



For CSA's Cloud Incident Response Working Group – Standards development – No reproduction or circulation"

Singapore Standards Council

TR 62 : 2018
(ICS 35.020; 35.210)

TECHNICAL REFERENCE

Guidelines for cloud outage incident response (COIR)

Published by

Enterprise Singapore

WG members come from:

asia cloud computing association · CSA cloud security alliance℠ · DSTA Defence Science & Technology Agency · ITMA IT Management Association · iTSC Information Technology Standards Committee · NUS National University of Singapore · SINGAPORE COMPUTER SOCIETY · SiTF · CSA APAC

COIR SCOPE

Within Scope

Cloud outages directly associated with:

- **Operational mistakes;**
- **Infrastructure or system failure;**
- **Environment issues** (like flooding/fire)

Out of Scope

Cyber-security incidents & malicious acts

Who Benefits?

Cloud Users

Transparency of service provided by CSPs

CSPs

Aligned to market demand on the services expectation

COIR Framework Overview

4 categories were defined in the COIR framework **based on impact of outage** to business, sector, economy and human life

Minimal Impact

Category D

For cloud services that are **least important** to an organisation's ops.

Alternative means/fallback mechanisms are available. Duration of outage in days is tolerable. Low urgency to access data during outage period

Operational Impact

Category C

For cloud services that are **essential** to an organisation's ops.

Ops restored within same day. Medium urgency to access data during outage period. Else outage will impact org's ops efficiency/ effectiveness significantly.

Business Critical Impact

Category B

For cloud services that are **critical** to an org's ops. Any outage can **impact biz severely**

Ops shall be restored within hours. Have a high urgency to access data during this period. Else, survival is at stake if outage prolongs

Systemic/ Mission Critical Impact

Category A

For cloud services that are **mission or safety critical** or affect stability of economy, mkt, industry (systemic).

The impact is beyond organisation's ops. Any outage will put human safety/stability of market, economy or industry at stake.

COIR Framework - Parameters

16 parameters (in 5 groups) for COIR categories

Availability & Resiliency

1. Availability %
2. Historic Record of Availability
3. Recovery Time Objective (RTO)
4. Recovery Point Objective (RPO)

Response Plan

9. Sharing of CSP’s COIR Plan
10. Exercise of CSP’s COIR Plan

Outage Handling

11. Notification Time of Cloud Outage Incident
12. Comm Channel Used for Notification of Cloud Outage Incident
13. Comm Channel Used by CSC to Report Cloud Outage Incident
14. Response Time by CSP
15. Frequency Of Status Update of Reported Outage
16. Channel of Comm Used for Status Update

Health Monitoring

7. Monitoring of Cloud Service Health by CSP
8. CSPs to Cloud Users for Health Monitoring of Cloud Services

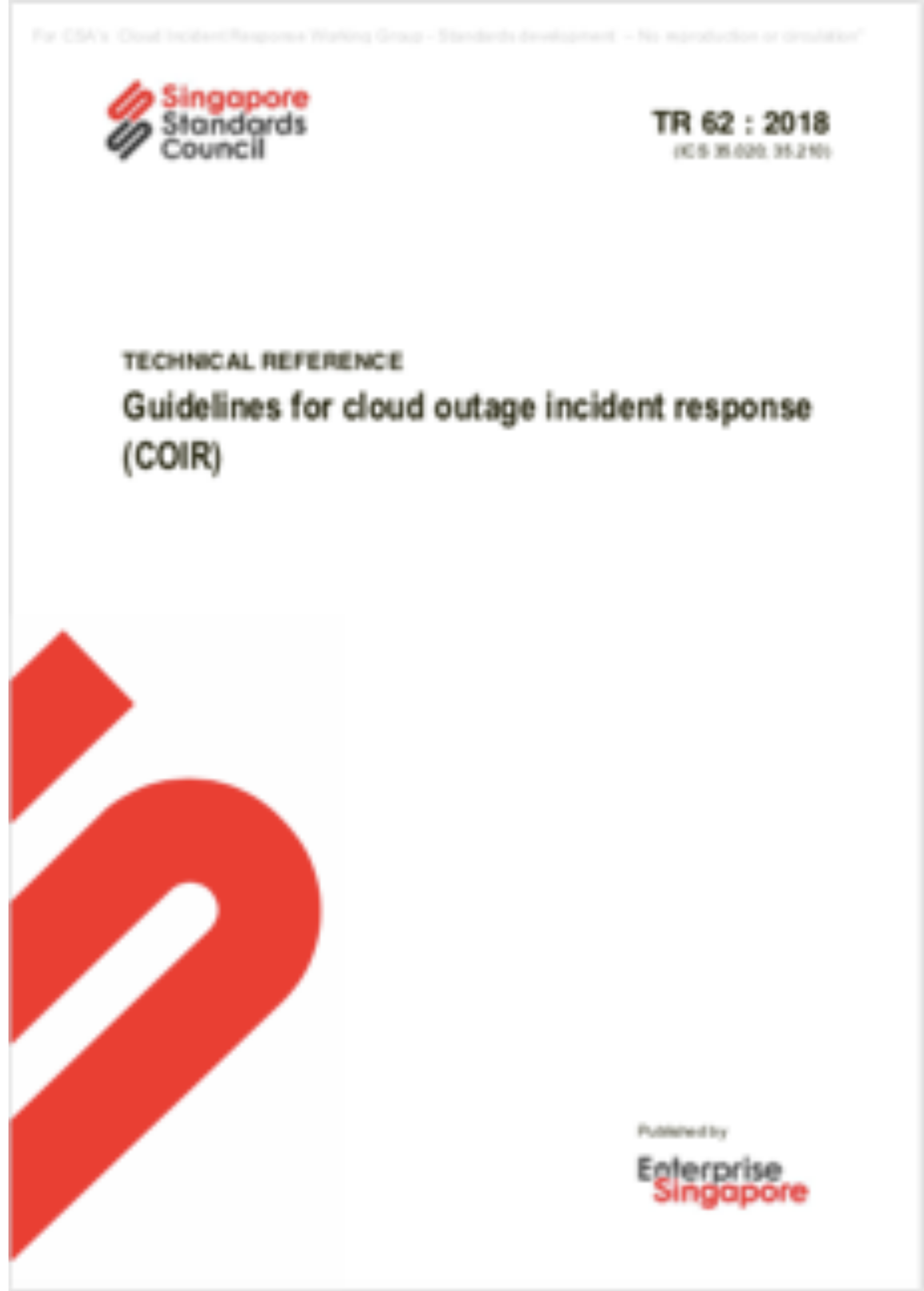
Support & Planned Maintenance

5. Support Hours

6a. Notification of Planned Maintenance to Cloud Users

6b. Notification Lead Time of Planned Maintenance

Gap to Bridge



For CSA's 'Cloud Incident Response Working Group – Standards development' – No reproduction or circulation'

Singapore Standards Council

TR 62 : 2018
(ICS 35.020; 35.210)

TECHNICAL REFERENCE
Guidelines for cloud outage incident response (COIR)

Published by
Enterprise Singapore

TR 62 - Cloud Outage Incident Response

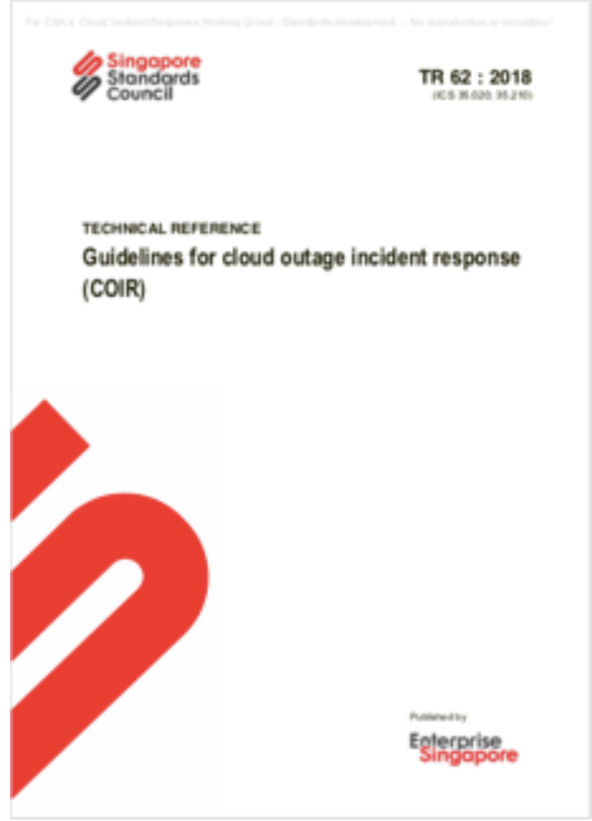
Out of Scope

Cyber-security incidents & malicious acts, previously out of scope in TR 62

Cloud incidents that do not involve outages but may impact regular operations, for e.g.

- Data breaches
- Misconfigurations

Cloud Incident Response (CIR)



Singapore Standards Council

TR 62 : 2018

TECHNICAL REFERENCE

Guidelines for cloud outage incident response (COIR)

Published by Enterprise Singapore

TR 62 - Cloud Outage Incident Response

SECURITY GUIDANCE

For Critical Areas of Focus In Cloud Computing v4.0

CSA Security Guidance v4.0 (Domain 9 Incident Response)

INTERNATIONAL STANDARD

ISO/IEC 27035-2

Information technology — Security techniques — Information security incident management —

Part 2: Guidelines to plan and prepare for incident response

ISO 27035 Information Security Incident Management

Cloud Computing

Benefits, risks and recommendations for information security

ENISA Cloud Computing Security Risk Assessment

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Special Publication 800-61 Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

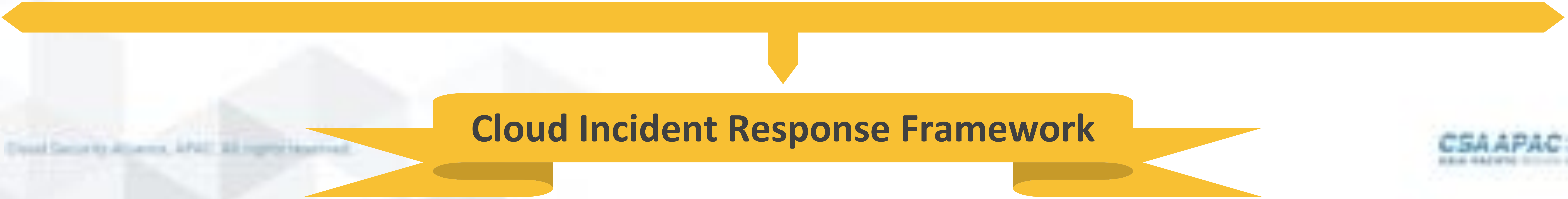
Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

NIST - Computer Security Incident Handling Guide

+ Other relevant documents suggested by WG members:

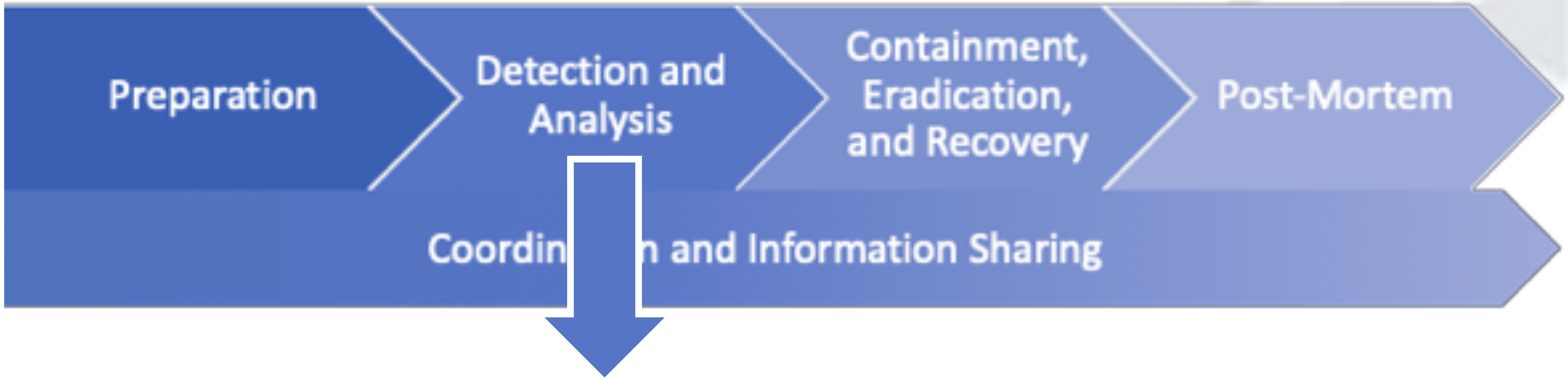
- ISO 223220:2011 Societal Security
- FedRAMP Incident Communications Procedure



Cloud Incident Response Framework

Deliverable: CIR Framework

SCOPE



Preparation

Detection and Analysis

Containment, Eradication, and Recovery

Post-Mortem

Coordin n and Information Sharing

4.2 Detection and Analysis

4.2.1 Inducement

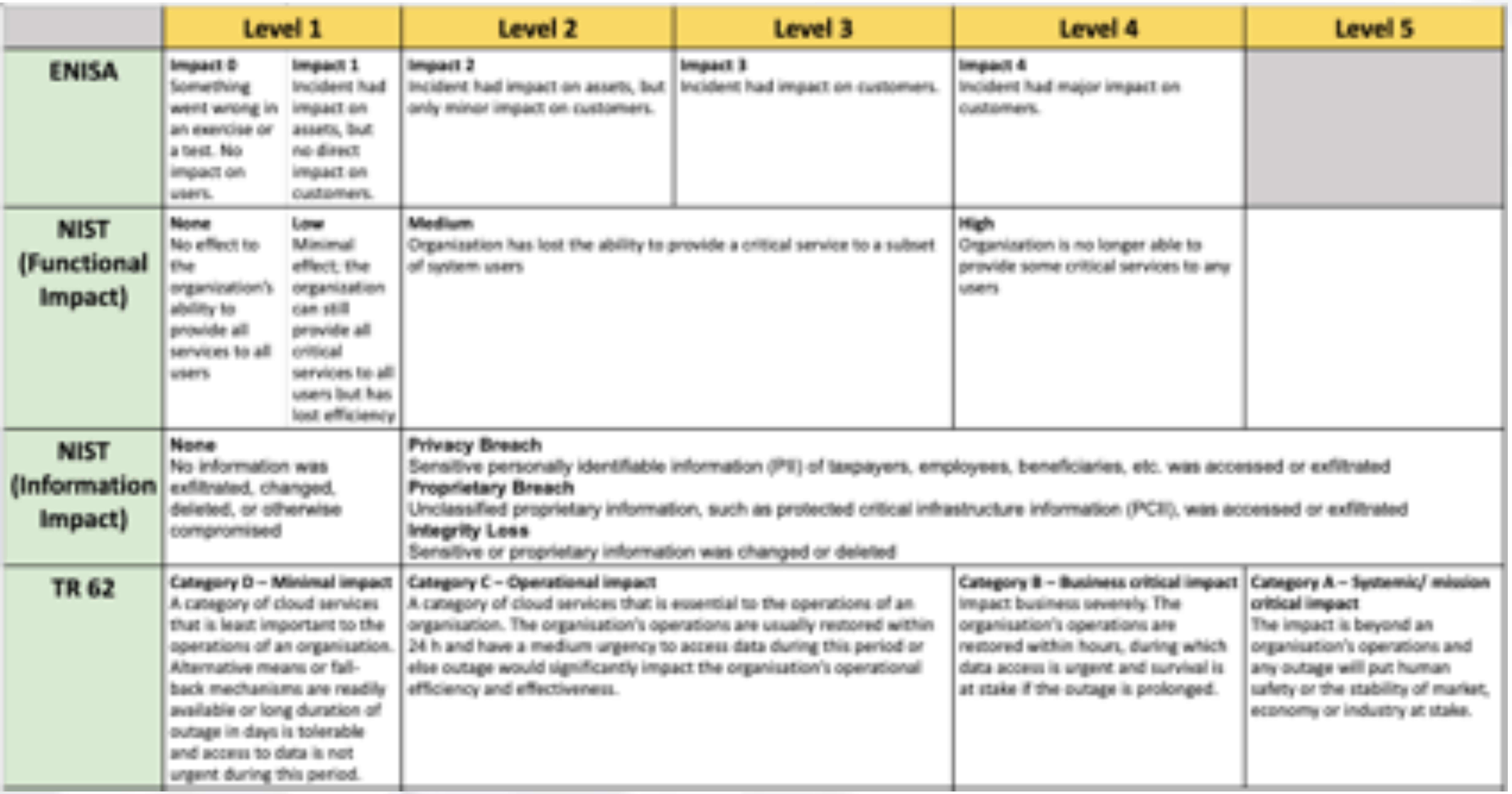
…

4.2.2 Incident Classification Scale

…

Deliverable: CIR Framework

INCIDENT CLASSIFICATION SCALE



	Level 1	Level 2	Level 3	Level 4	Level 5
ENISA	**Impact 0** Something went wrong in an exercise or a test. No impact on users. **Impact 1** Incident had impact on assets, but no direct impact on customers.	**Impact 2** Incident had impact on assets, but only minor impact on customers.	**Impact 3** Incident had impact on customers.	**Impact 4** Incident had major impact on customers.	
NIST (Functional Impact)	**None** No effect to the organization's ability to provide all services to all users **Low** Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	**Medium** Organization has lost the ability to provide a critical service to a subset of system users		**High** Organization is no longer able to provide some critical services to any users	
NIST (Information Impact)	**None** No information was exfiltrated, changed, deleted, or otherwise compromised	**Privacy Breach** Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated **Proprietary Breach** Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated **Integrity Loss** Sensitive or proprietary information was changed or deleted			
TR 62	**Category D – Minimal impact** A category of cloud services that is least important to the operations of an organisation. Alternative means or fall-back mechanisms are readily available or long duration of outage in days is tolerable and access to data is not urgent during this period.	**Category C – Operational impact** A category of cloud services that is essential to the operations of an organisation. The organisation's operations are usually restored within 24 h and have a medium urgency to access data during this period or else outage would significantly impact the organisation's operational efficiency and effectiveness.		**Category B – Business critical impact** Impact business severely. The organisation's operations are restored within hours, during which data access is urgent and survival is at stake if the outage is prolonged.	**Category A – Systemic/ mission critical impact** The impact is beyond an organisation's operations and any outage will put human safety or the stability of market, economy or industry at stake.

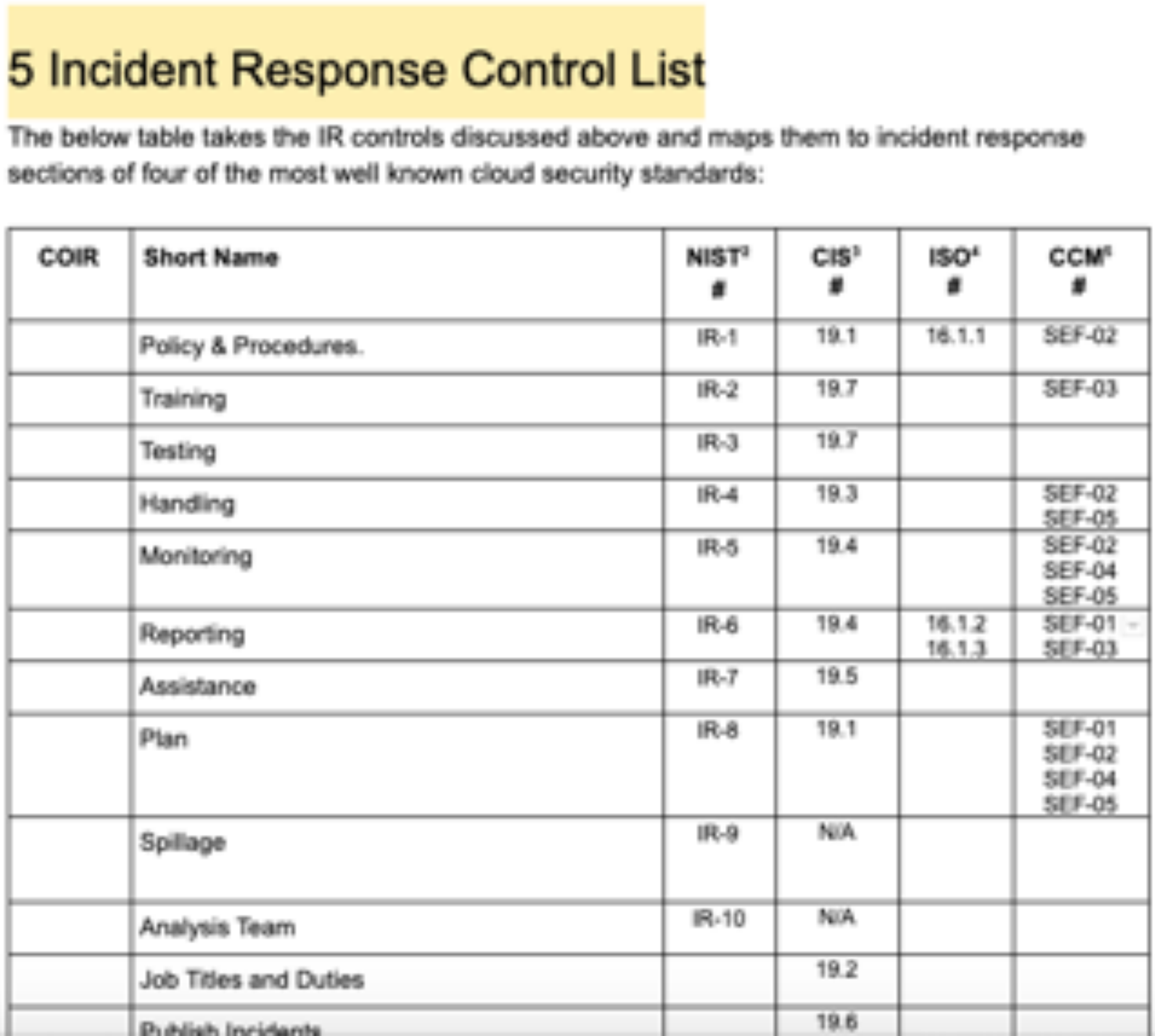
The Incident Classification Scale classifies incidents into 5 categories, from Level 1 to Level 5, with **increment of impact** at each level.

Severity of each level can be mapped to:

- ENISA Cloud Security Incident Reporting
- NIST Computer Security Incident Handling Guide (Functional and Information impact)
- TR 62 Guidelines for Cloud Outage Incident Response

Deliverable: CIR Framework

INCIDENT RESPONSE CONTROL LIST



5 Incident Response Control List

The below table takes the IR controls discussed above and maps them to incident response sections of four of the most well known cloud security standards:

COIR	Short Name	NIST[2] \#	CIS[3] \#	ISO[4] \#	CCM[5] \#
	Policy & Procedures.	IR-1	19.1	16.1.1	SEF-02
	Training	IR-2	19.7		SEF-03
	Testing	IR-3	19.7		
	Handling	IR-4	19.3		SEF-02 SEF-05
	Monitoring	IR-5	19.4		SEF-02 SEF-04 SEF-05
	Reporting	IR-6	19.4	16.1.2 16.1.3	SEF-01 SEF-03
	Assistance	IR-7	19.5		
	Plan	IR-8	19.1		SEF-01 SEF-02 SEF-04 SEF-05
	Spillage	IR-9	N/A		
	Analysis Team	IR-10	N/A		
	Job Titles and Duties		19.2		
	Publish Incidents		19.6		

WG members can contribute by proposing new ideas / chapters to consider.

This Incident Response Control List is volunteer-proposed and -developed chapter.

The list maps controls that were discussed in the framework to incident response sections of 4 of the most well known cloud security standards & guidelines, namely:

1. NIST
2. CIS
3. ISO
4. CSA's Cloud Controls Matrix (CCM)

CIR WG

CURRENT STATUS

EXECUTION

Cloud Incident Response Framework

In process of working with WG co-chairs and members to develop outline of the deliverable. Beefing up scope and structure.

Next phase: OPEN PEER REVIEW

- **+ CIR WG Charter:** *CLICK HERE*
- **+ CIR Framework Draft:** *CLICK HERE*
- **+ Volunteers' Responsibility:** *CLICK HERE*

CSA welcomes any domain experts to join the WG.

CIR WG

COMPOSITION

LEADERSHIP

- Soon Tein LIM
- Prof. Alex SIOW

COMPANIES REPRESENTED

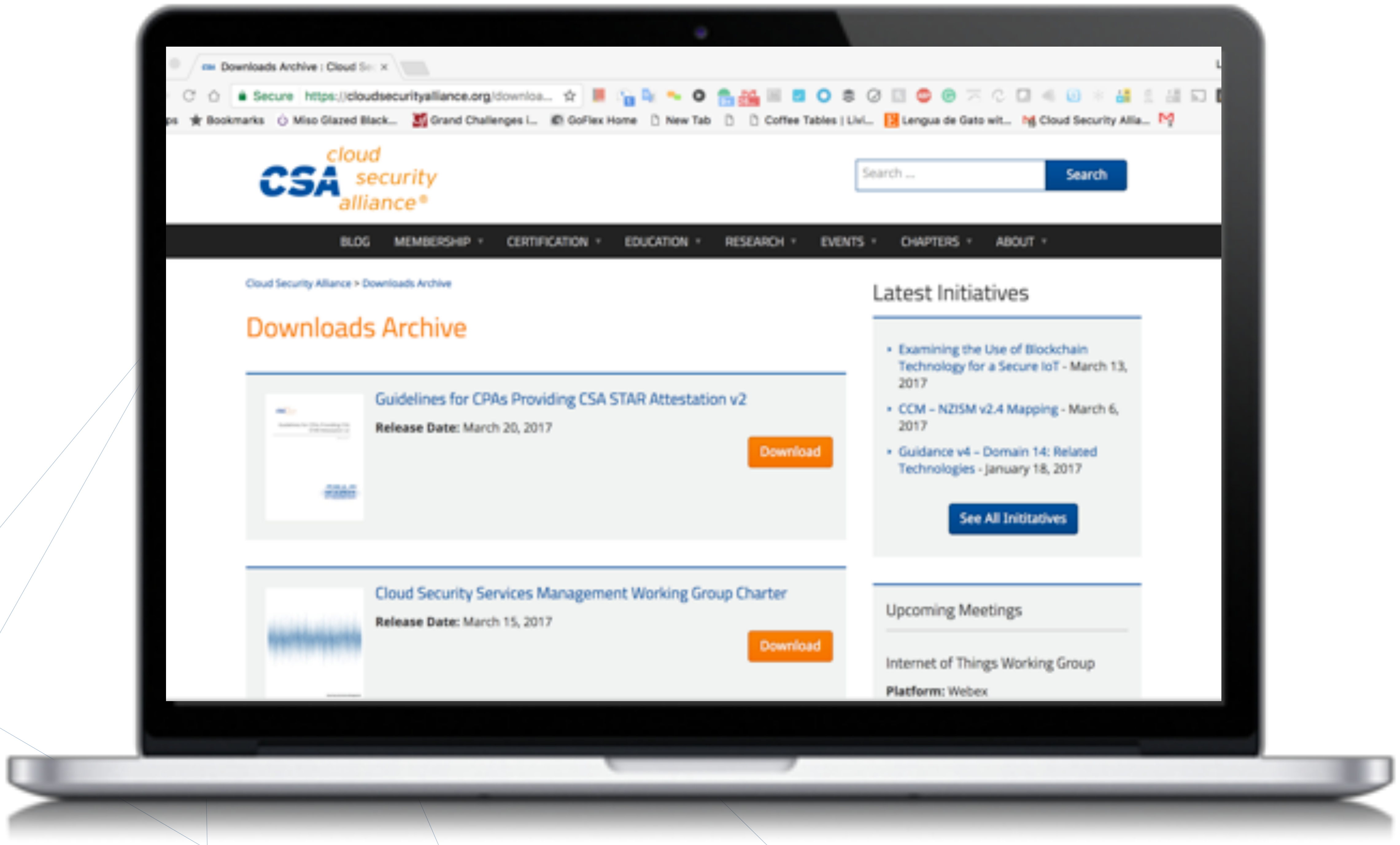
- TROPOSPHERE TECH
- UBER TECHNOLOGIES
- OPUS CONSULTING GROUP
- ONE ESECURITY
- LGMS
- DELOITTE
- MNIT AN IN
- FEDERAL RESERVE BANK
- UPMC
- CYBER RESCUE
- ST ENGINEERING
- DATAGSP
- DGA
- WIPRO LTD
- ORMGT
- RESOLVO

Like to Join the CSA CIR Working Group?

Please go to:

https://cloudsecurityalliance.org/working-groups/cloud-incident-response/#_join

THANK YOU



Cloud Security Alliance > Downloads Archive

Downloads Archive

Guidelines for CPAs Providing CSA STAR Attestation v2

Release Date: March 20, 2017

Cloud Security Services Management Working Group Charter

Release Date: March 15, 2017

Latest Initiatives

- Examining the Use of Blockchain Technology for a Secure IoT - March 13, 2017
- CCM – NZISM v2.4 Mapping - March 6, 2017
- Guidance v4 – Domain 14: Related Technologies - January 18, 2017

Upcoming Meetings

Internet of Things Working Group

Platform: Webex

Contact CSA

Email: csa-apac-research@cloudsecurityalliance.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org

Learn: www.cloudsecurityalliance.org/research/cloudbytes

Download: www.cloudsecurityalliance.org/download

GDPR Resource center: https://gdpr.cloudsecurityalliance.org