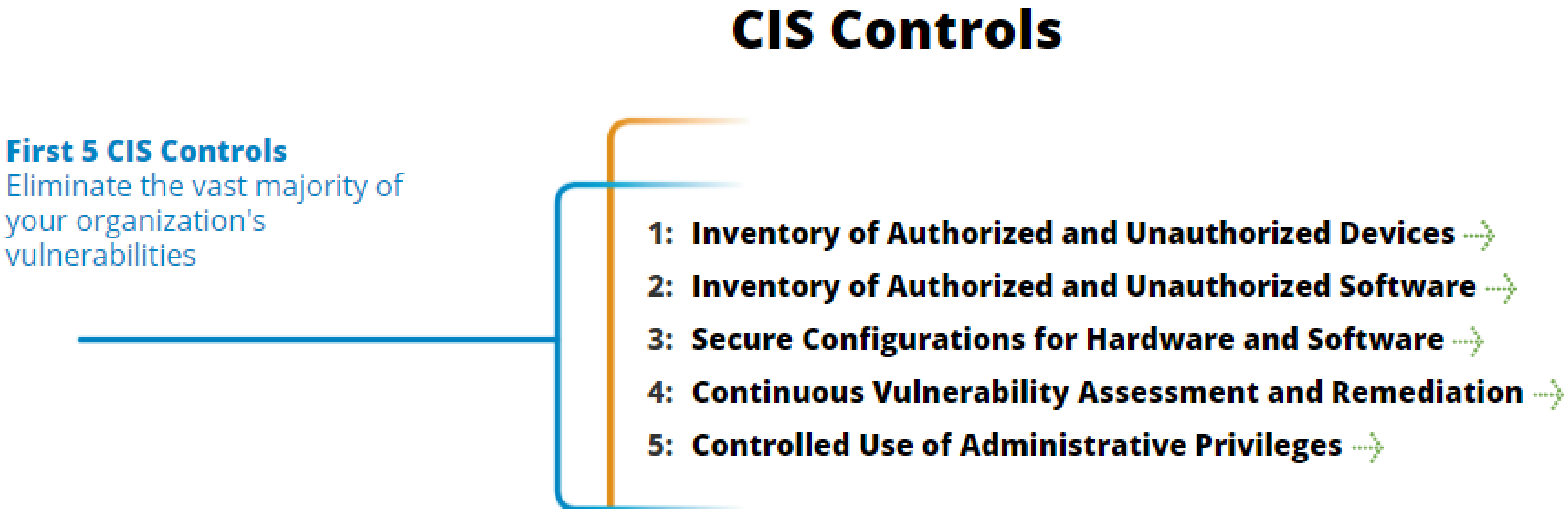
Everything you save CAN and WILL be used against you in the event of a breach

Department of Innovation and Technology

George Khalil, Chief Information Security Officer

CSMFO Annual Conference

CIS 20 Critical Controls



CIS Controls

First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

1: **Inventory of Authorized and Unauthorized Devices**

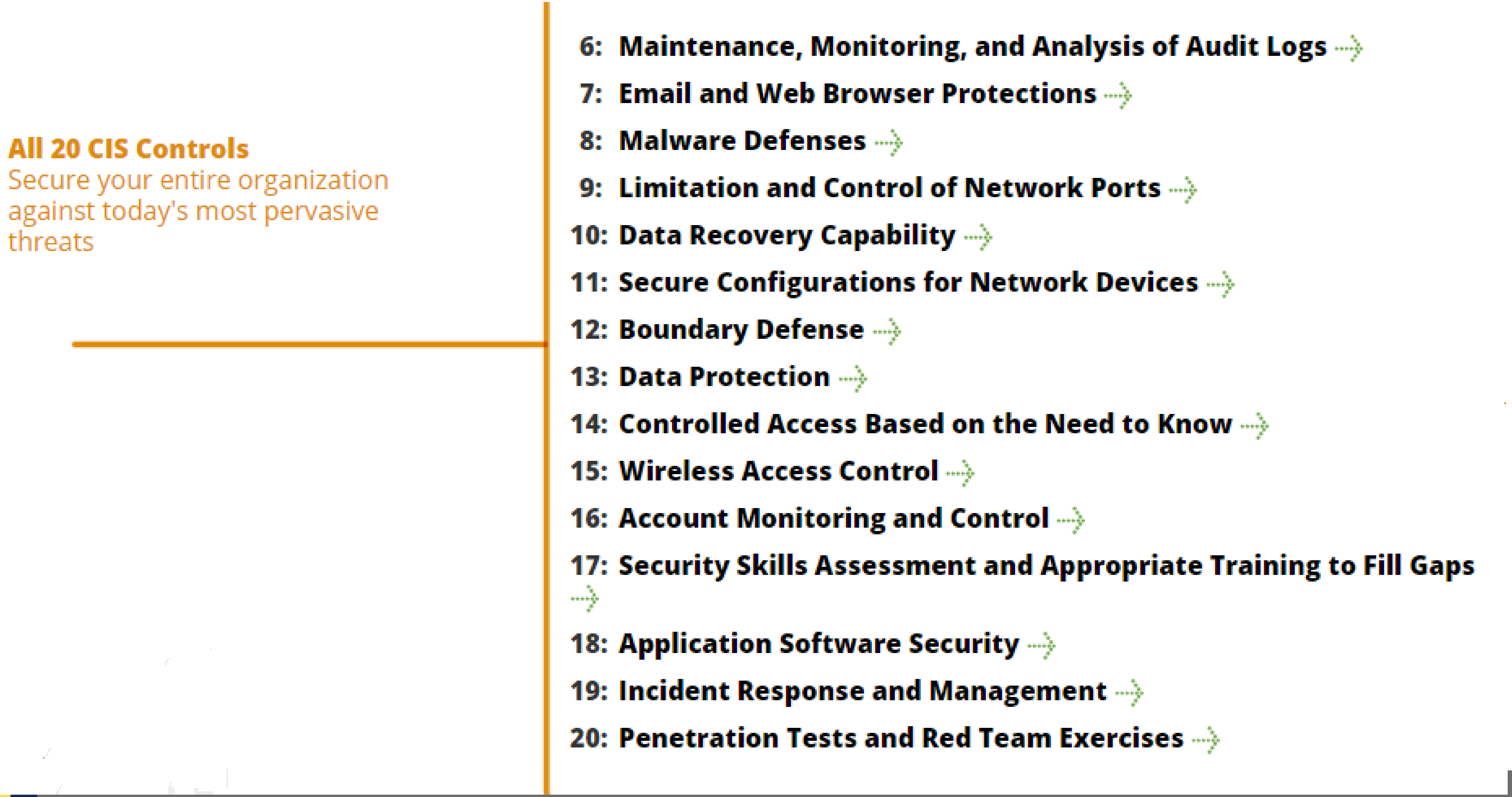
2: **Inventory of Authorized and Unauthorized Software**

3: **Secure Configurations for Hardware and Software**

4: **Continuous Vulnerability Assessment and Remediation**

5: **Controlled Use of Administrative Privileges**

CIS 20 Critical Controls



All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: Maintenance, Monitoring, and Analysis of Audit Logs

7: Email and Web Browser Protections

8: Malware Defenses

9: Limitation and Control of Network Ports

10: Data Recovery Capability

11: Secure Configurations for Network Devices

12: Boundary Defense

13: Data Protection

14: Controlled Access Based on the Need to Know

15: Wireless Access Control

16: Account Monitoring and Control

17: Security Skills Assessment and Appropriate Training to Fill Gaps

18: Application Software Security

19: Incident Response and Management

20: Penetration Tests and Red Team Exercises

Pervasive Threats?

CIS Control 13

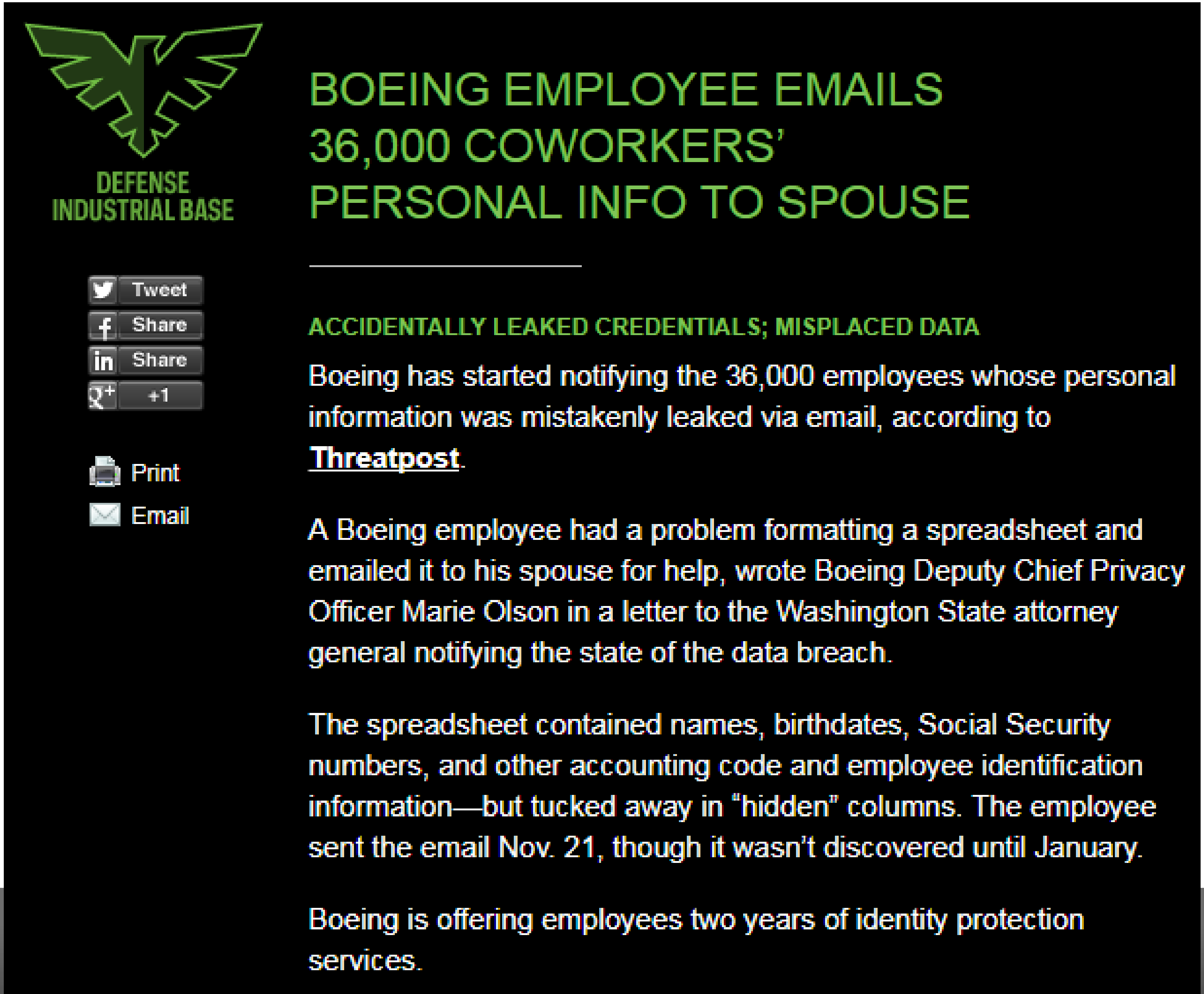
Data Protection

- Key Principle:
- The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

Pervasive Threats?

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data are leaked or lost as a result of theft or espionage, **the vast majority of these problems result from poorly understood data practices**, a **lack of effective policy architectures, and user error**. Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

Pervasive Threats?



BOEING EMPLOYEE EMAILS 36,000 COWORKERS' PERSONAL INFO TO SPOUSE

ACCIDENTALLY LEAKED CREDENTIALS; MISPLACED DATA

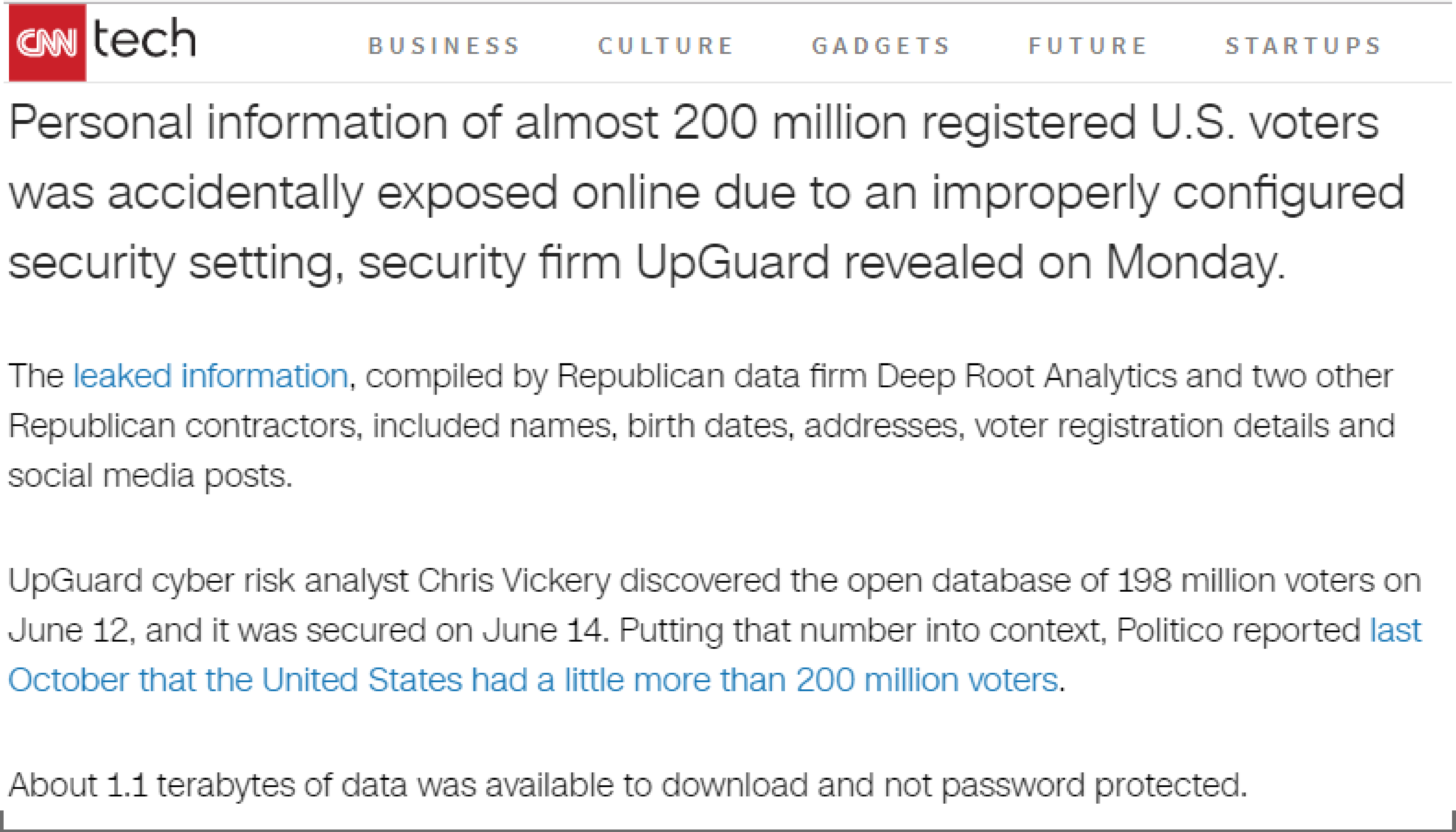
Boeing has started notifying the 36,000 employees whose personal information was mistakenly leaked via email, according to **Threatpost**.

A Boeing employee had a problem formatting a spreadsheet and emailed it to his spouse for help, wrote Boeing Deputy Chief Privacy Officer Marie Olson in a letter to the Washington State attorney general notifying the state of the data breach.

The spreadsheet contained names, birthdates, Social Security numbers, and other accounting code and employee identification information—but tucked away in "hidden" columns. The employee sent the email Nov. 21, though it wasn't discovered until January.

Boeing is offering employees two years of identity protection services.

Pervasive Threats?



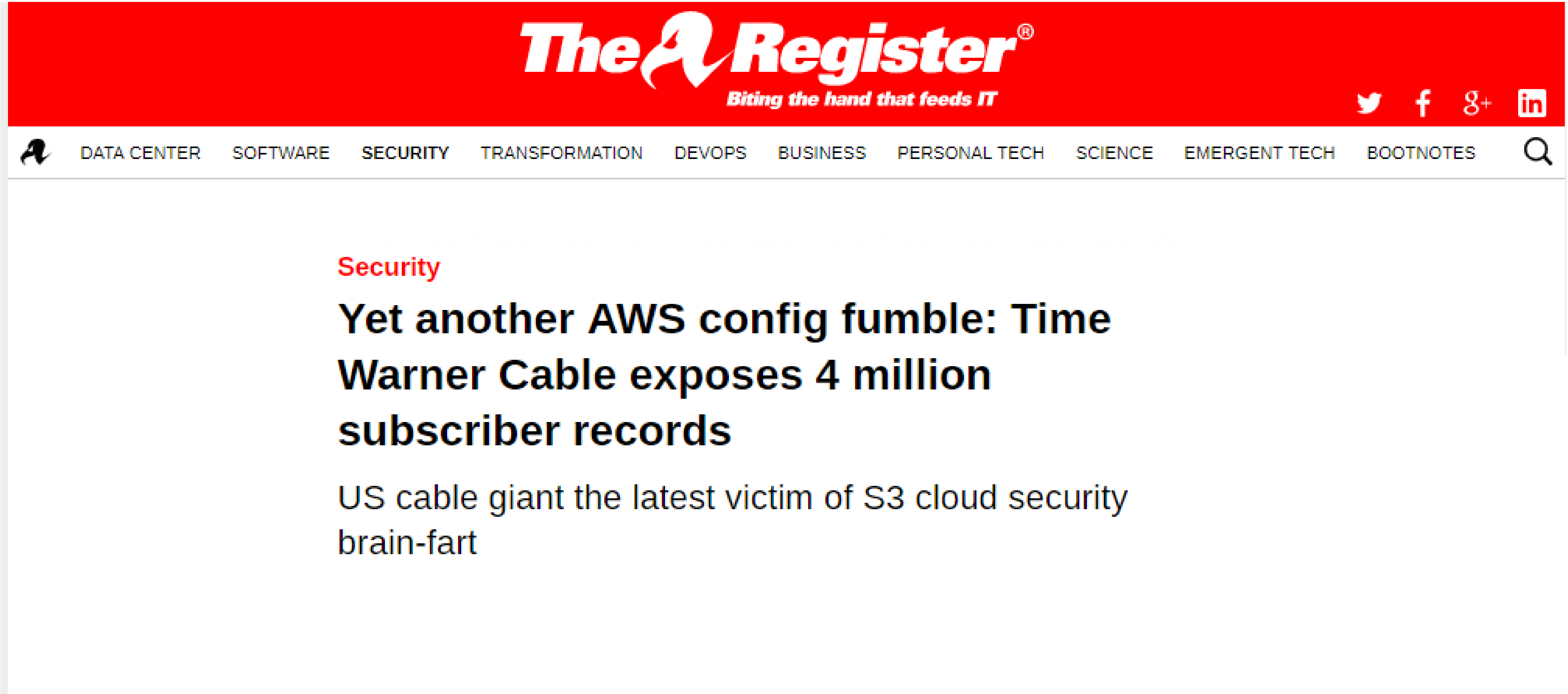
Personal information of almost 200 million registered U.S. voters was accidentally exposed online due to an improperly configured security setting, security firm UpGuard revealed on Monday.

The leaked information, compiled by Republican data firm Deep Root Analytics and two other Republican contractors, included names, birth dates, addresses, voter registration details and social media posts.

UpGuard cyber risk analyst Chris Vickery discovered the open database of 198 million voters on June 12, and it was secured on June 14. Putting that number into context, Politico reported last October that the United States had a little more than 200 million voters.

About 1.1 terabytes of data was available to download and not password protected.

Pervasive Threats?

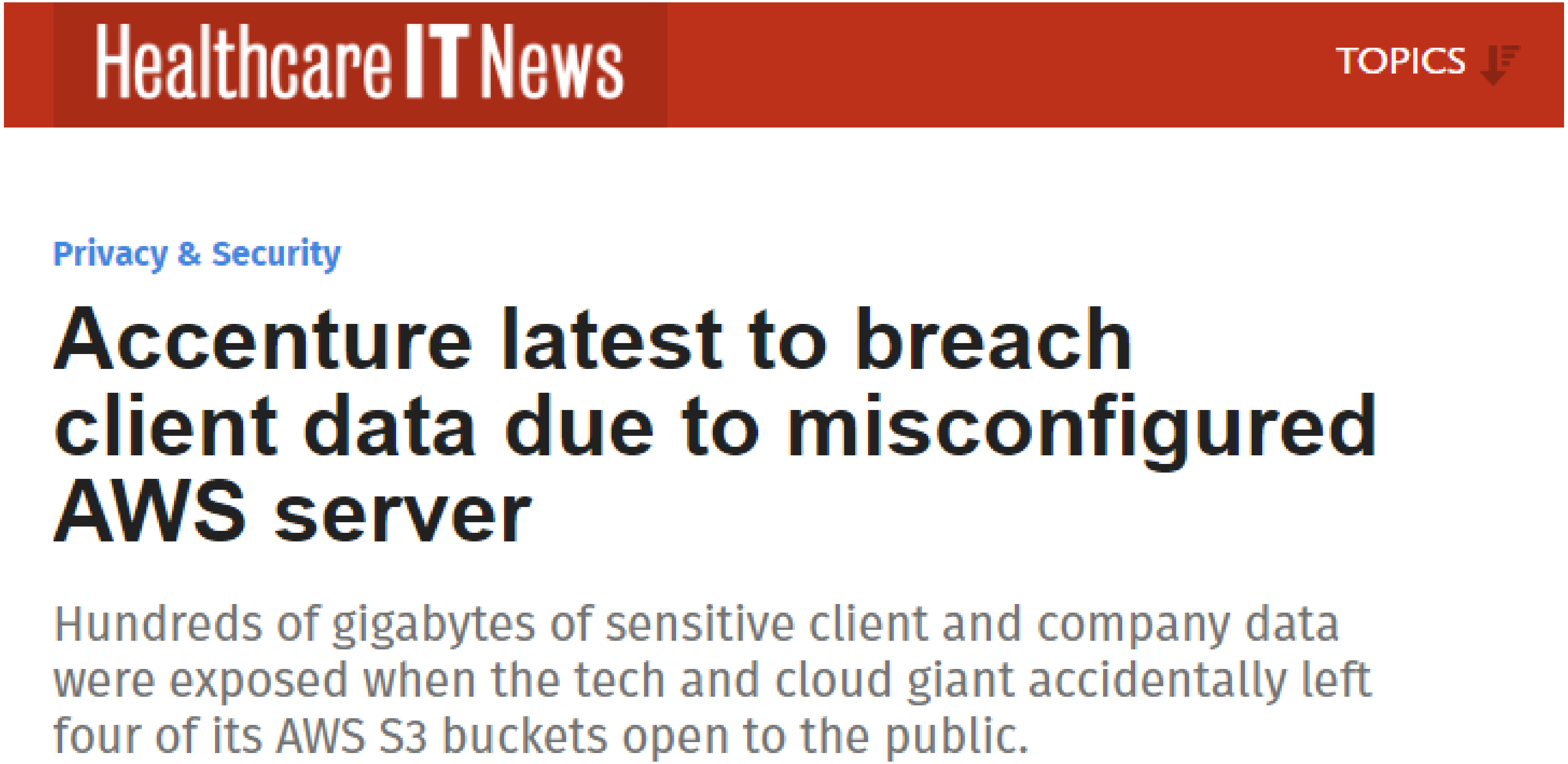


Security

Yet another AWS config fumble: Time Warner Cable exposes 4 million subscriber records

US cable giant the latest victim of S3 cloud security brain-fart

Pervasive Threats?



Healthcare IT News

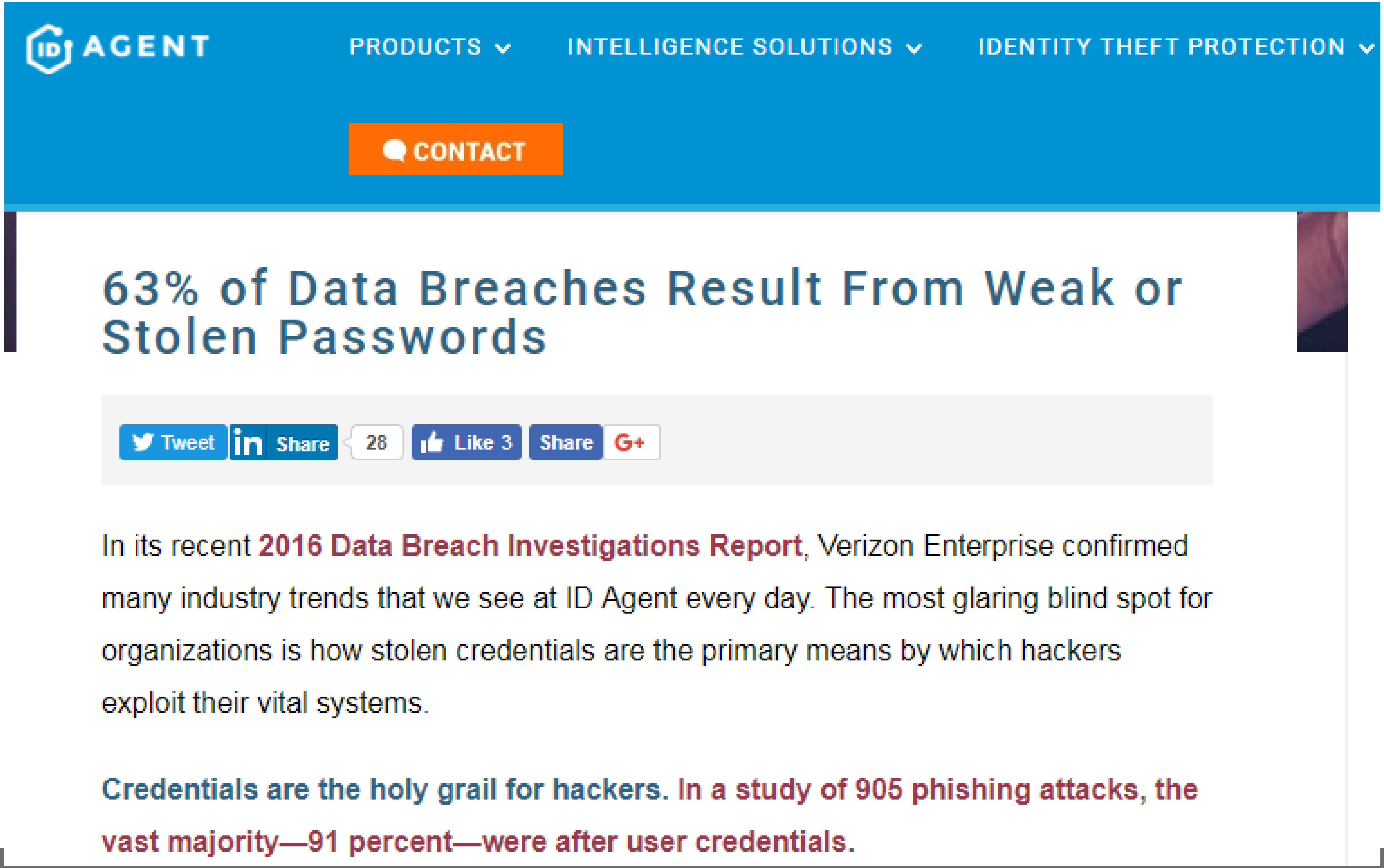
TOPICS

Privacy & Security

Accenture latest to breach client data due to misconfigured AWS server

Hundreds of gigabytes of sensitive client and company data were exposed when the tech and cloud giant accidentally left four of its AWS S3 buckets open to the public.

Pervasive Threats?

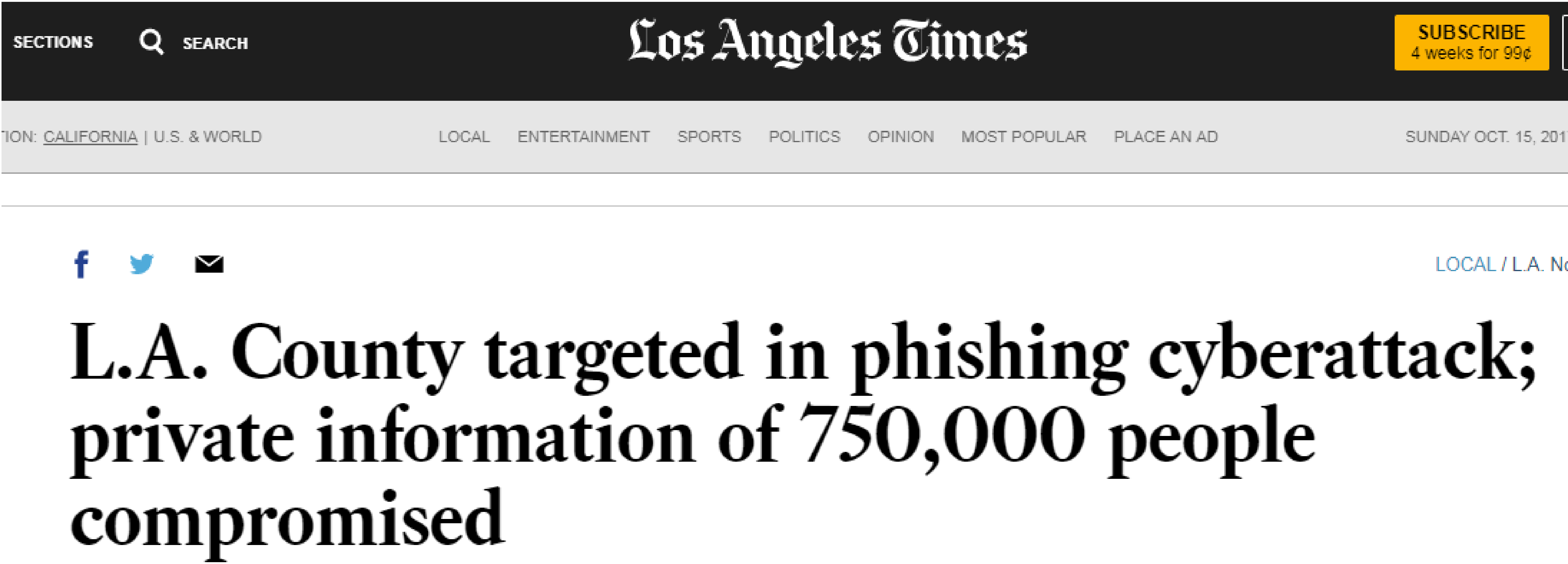


63% of Data Breaches Result From Weak or Stolen Passwords

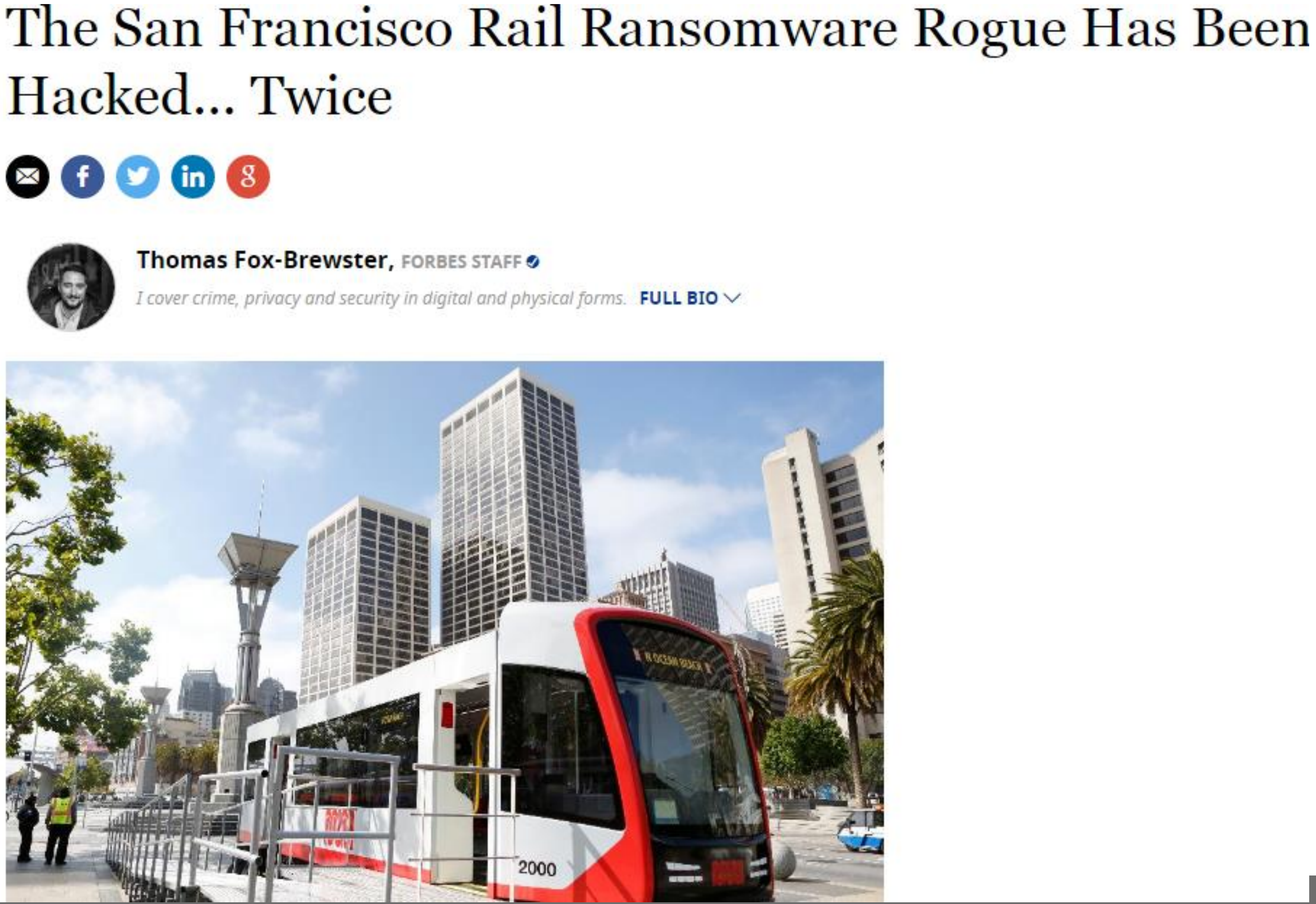
In its recent **2016 Data Breach Investigations Report**, Verizon Enterprise confirmed many industry trends that we see at ID Agent every day. The most glaring blind spot for organizations is how stolen credentials are the primary means by which hackers exploit their vital systems.

Credentials are the holy grail for hackers. In a study of 905 phishing attacks, the vast majority—91 percent—were after user credentials.

Pervasive Threats?



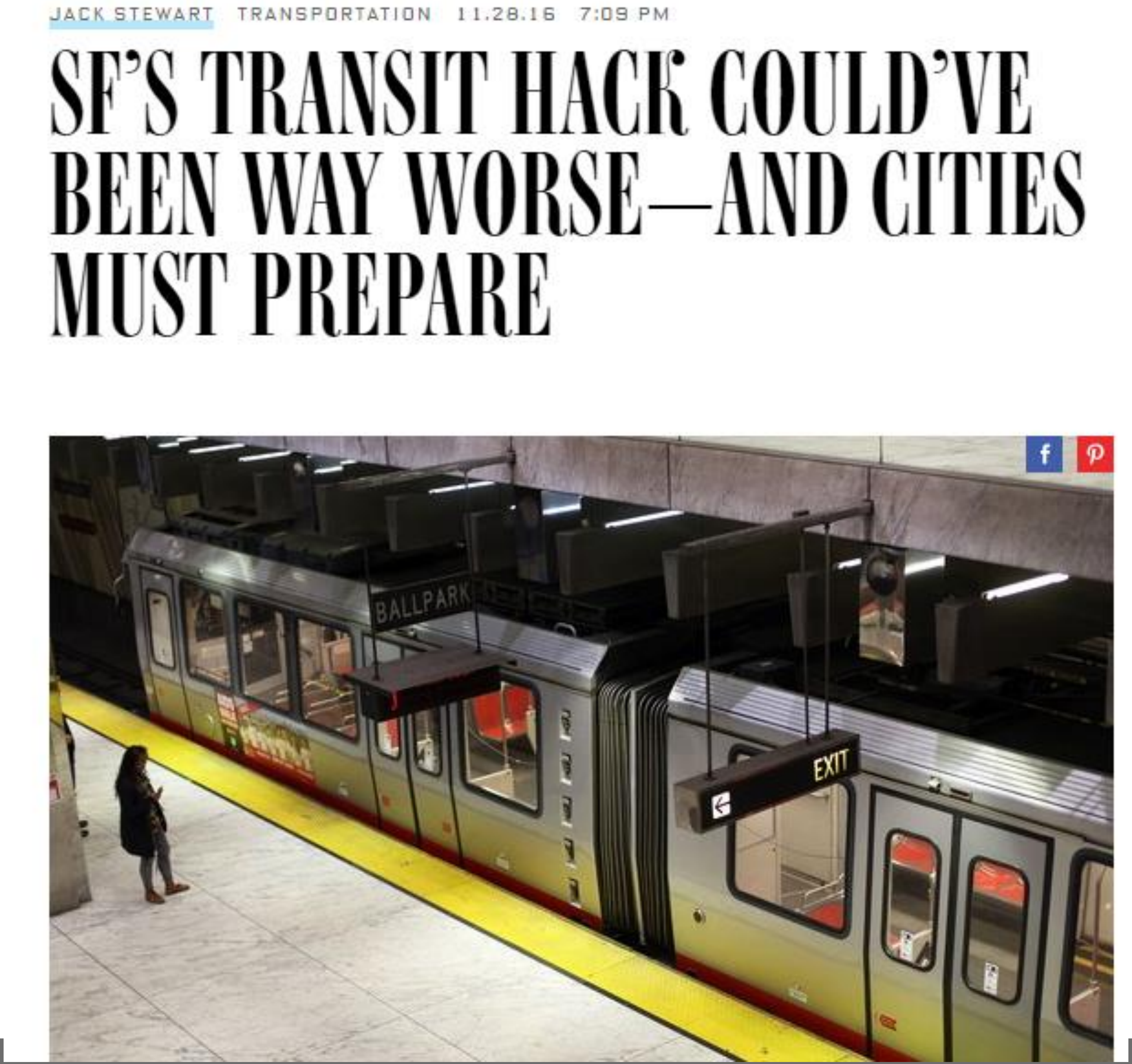
L.A. County targeted in phishing cyberattack; private information of 750,000 people compromised



The San Francisco Rail Ransomware Rogue Has Been Hacked... Twice

Thomas Fox-Brewster, FORBES STAFF

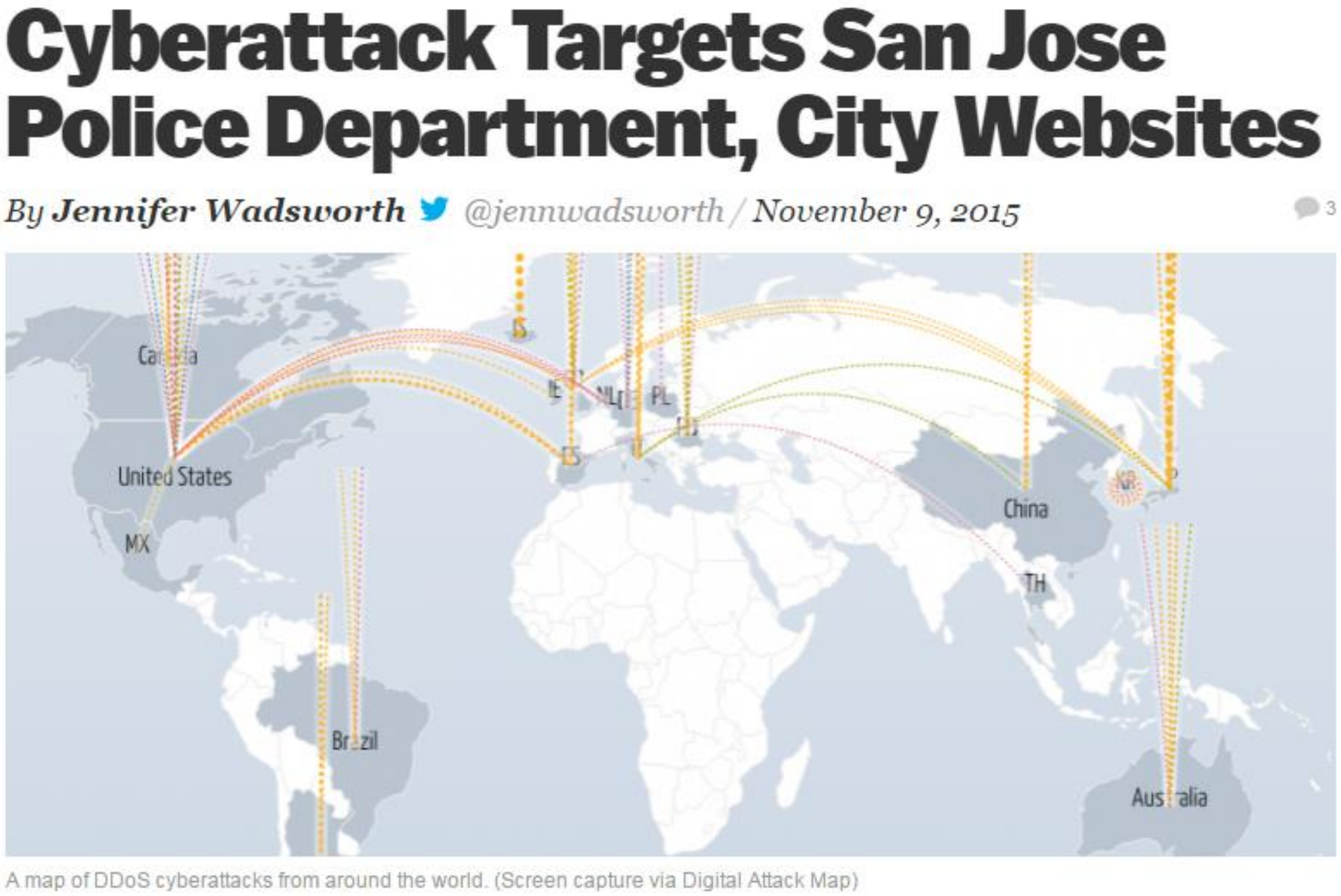
I cover crime, privacy and security in digital and physical forms. **FULL BIO**



JACK STEWART TRANSPORTATION 11.28.16 7:09 PM

SF'S TRANSIT HACK COULD'VE BEEN WAY WORSE—AND CITIES MUST PREPARE

"Muni would lose an estimated $559,000 for every day that it was unable to collect fares, according to its operating budget (see *Ransomware Extortion: A Question of Time*)."

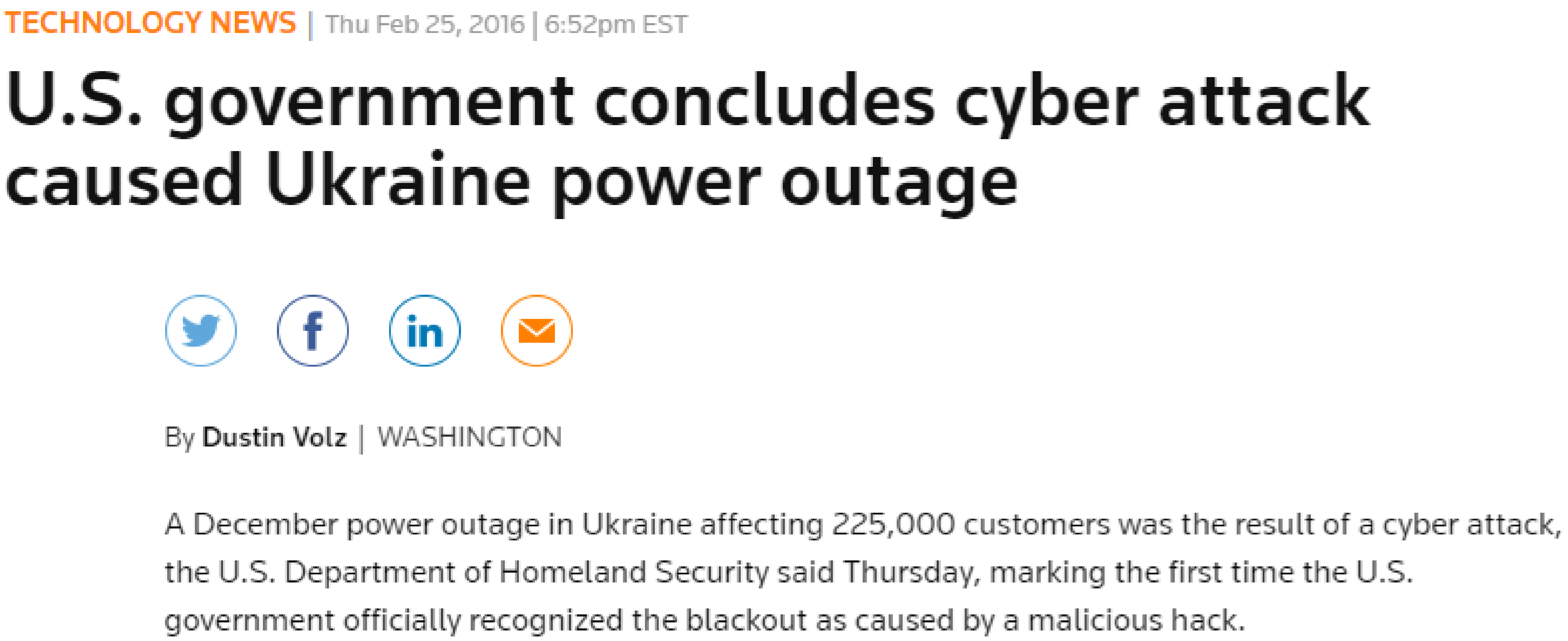


Cyberattack Targets San Jose Police Department, City Websites

*By **Jennifer Wadsworth** @jennwadsworth / November 9, 2015*

3

A map of DDoS cyberattacks from around the world. (Screen capture via Digital Attack Map)

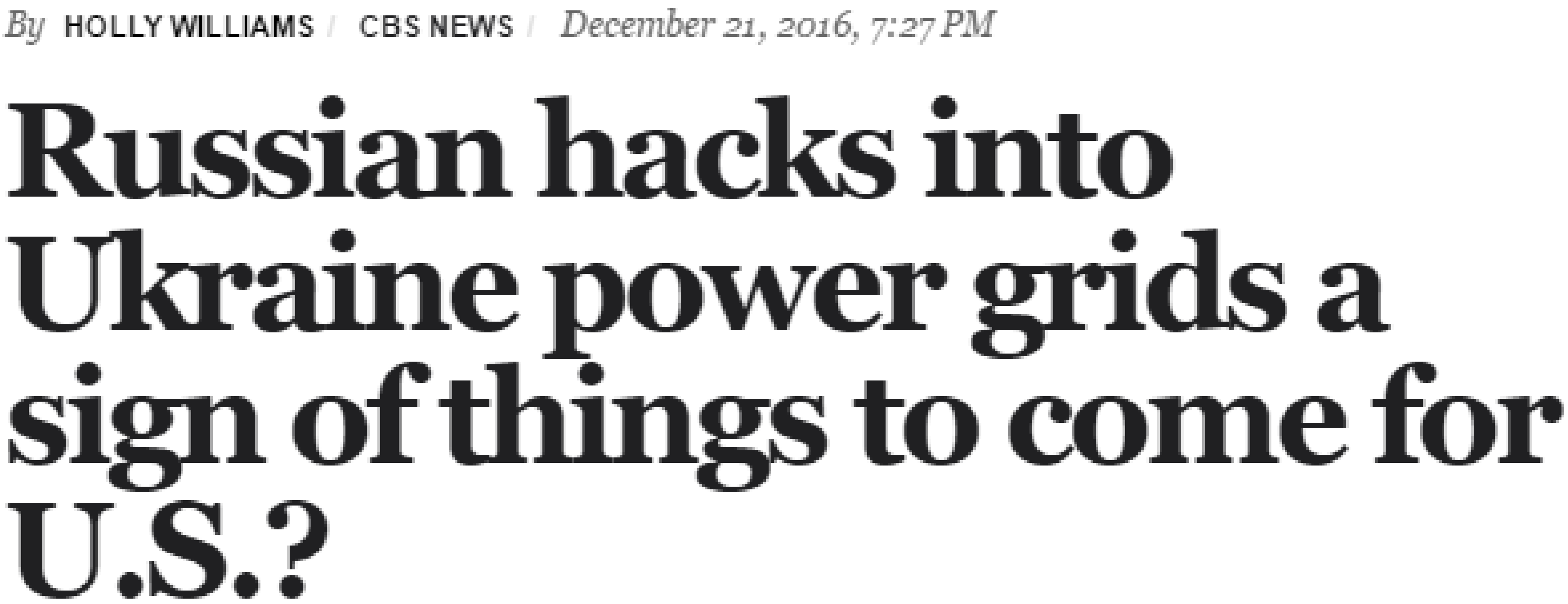


TECHNOLOGY NEWS | Thu Feb 25, 2016 | 6:52pm EST

U.S. government concludes cyber attack caused Ukraine power outage

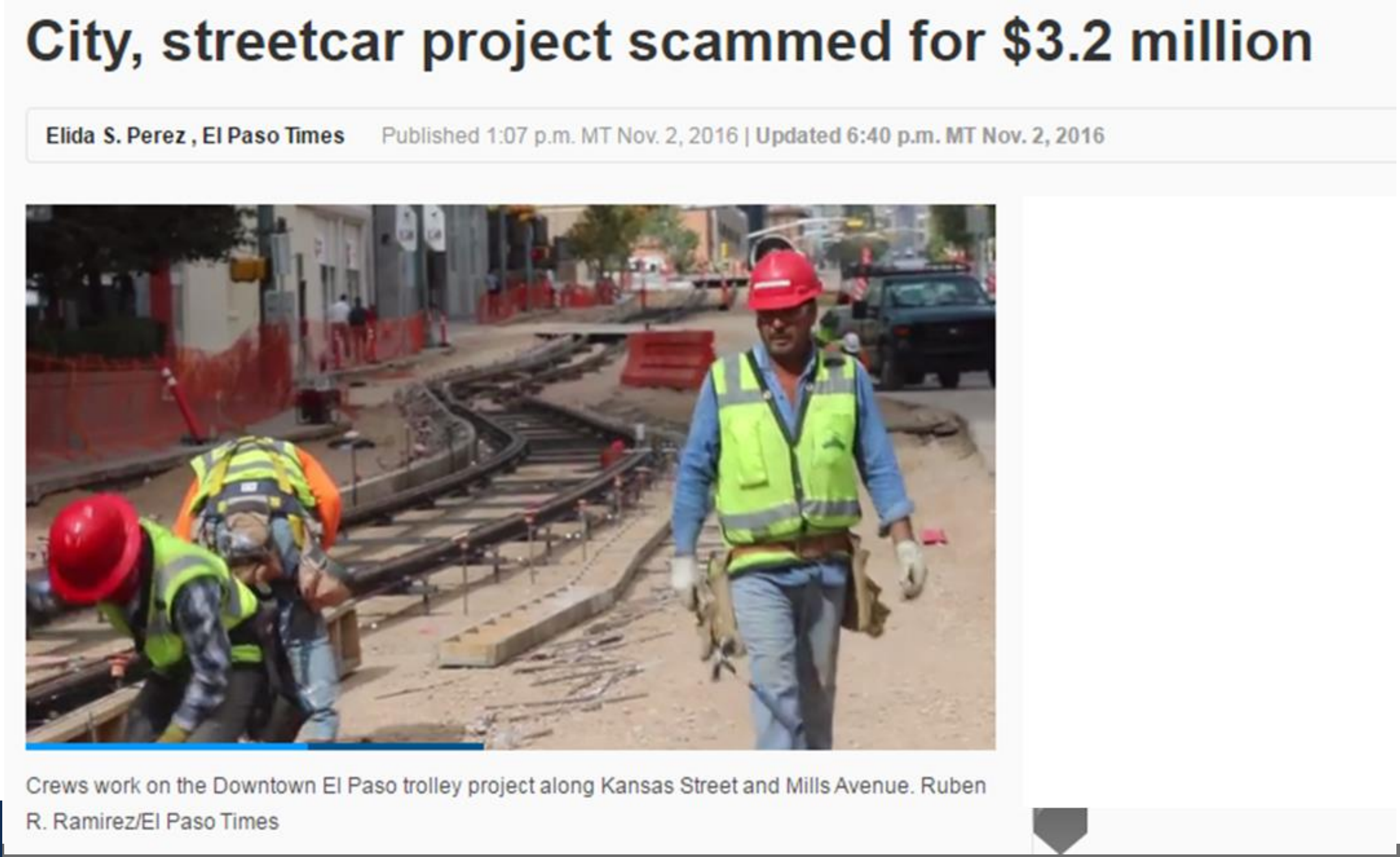
By **Dustin Volz** | WASHINGTON

A December power outage in Ukraine affecting 225,000 customers was the result of a cyber attack, the U.S. Department of Homeland Security said Thursday, marking the first time the U.S. government officially recognized the blackout as caused by a malicious hack.



By HOLLY WILLIAMS / CBS NEWS / December 21, 2016, 7:27 PM

Russian hacks into Ukraine power grids a sign of things to come for U.S.?

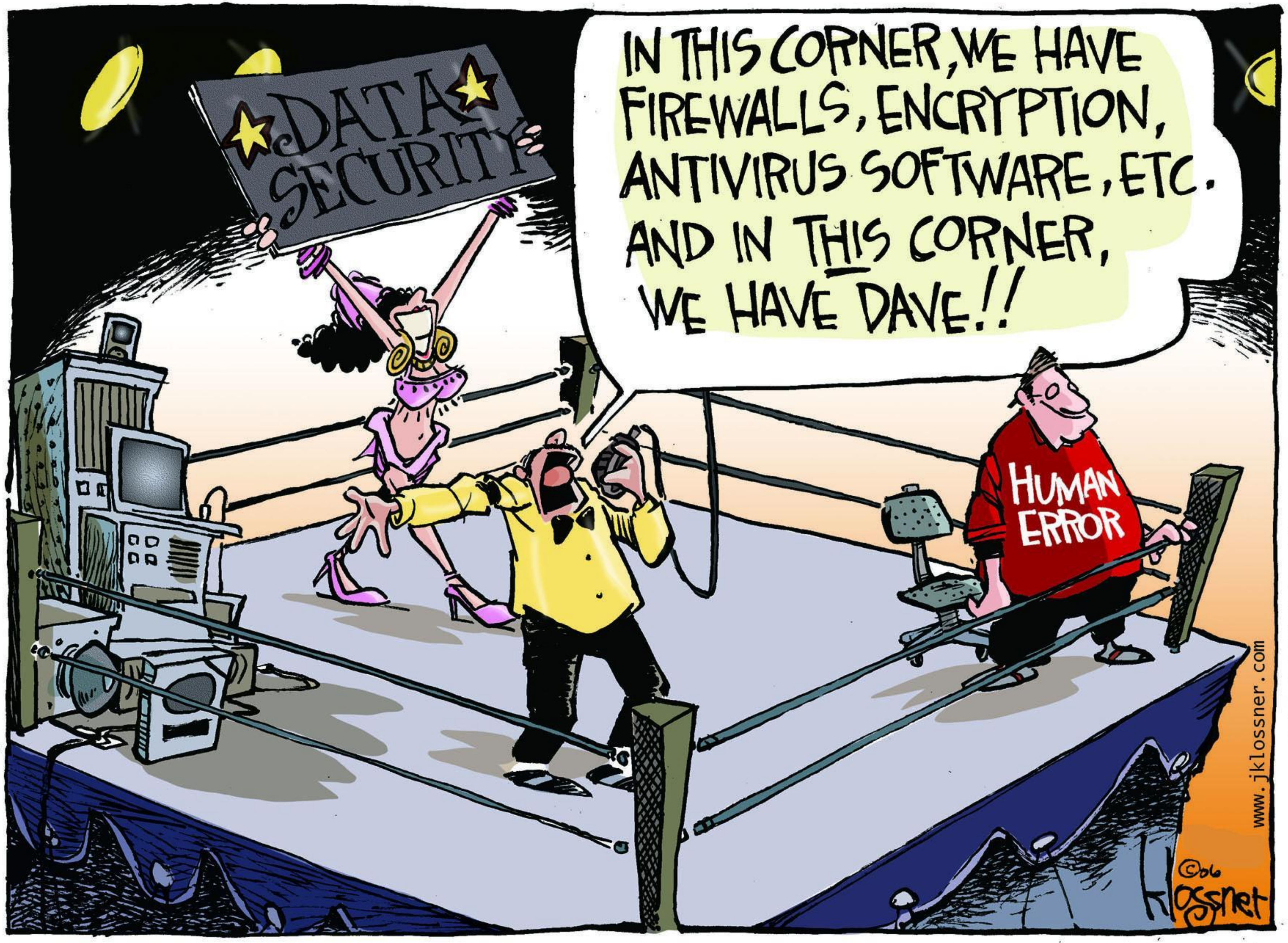


City, streetcar project scammed for $3.2 million

Elida S. Perez , El Paso Times Published 1:07 p.m. MT Nov. 2, 2016 | **Updated 6:40 p.m. MT Nov. 2, 2016**

Crews work on the Downtown El Paso trolley project along Kansas Street and Mills Avenue. Ruben R. Ramirez/El Paso Times

WHO HAS **ACCESS** TO YOUR DATA?


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
©06 klossner

copyright 2006 john klossner, www.jklossner.com

www.jklossner.com

What constitute protected data?

- PII (SSN, DL, Medical, Username and password, Credit card)
- **CIVIL CODE - CIV**
- **DIVISION 3. OBLIGATIONS [1427 - 3272.9]**
- *(Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.)*
- **PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273]**
- *(Part 4 enacted 1872.)*
- **TITLE 1.8. PERSONAL DATA [1798 - 1798.78]**
- *(Title 1.8 added by Stats. 1977, Ch. 709.)*
- **CHAPTER 1. Information Practices Act of 1977 [1798 - 1798.78]**
- *(Chapter 1 added by Stats. 1977, Ch. 709.)*
-

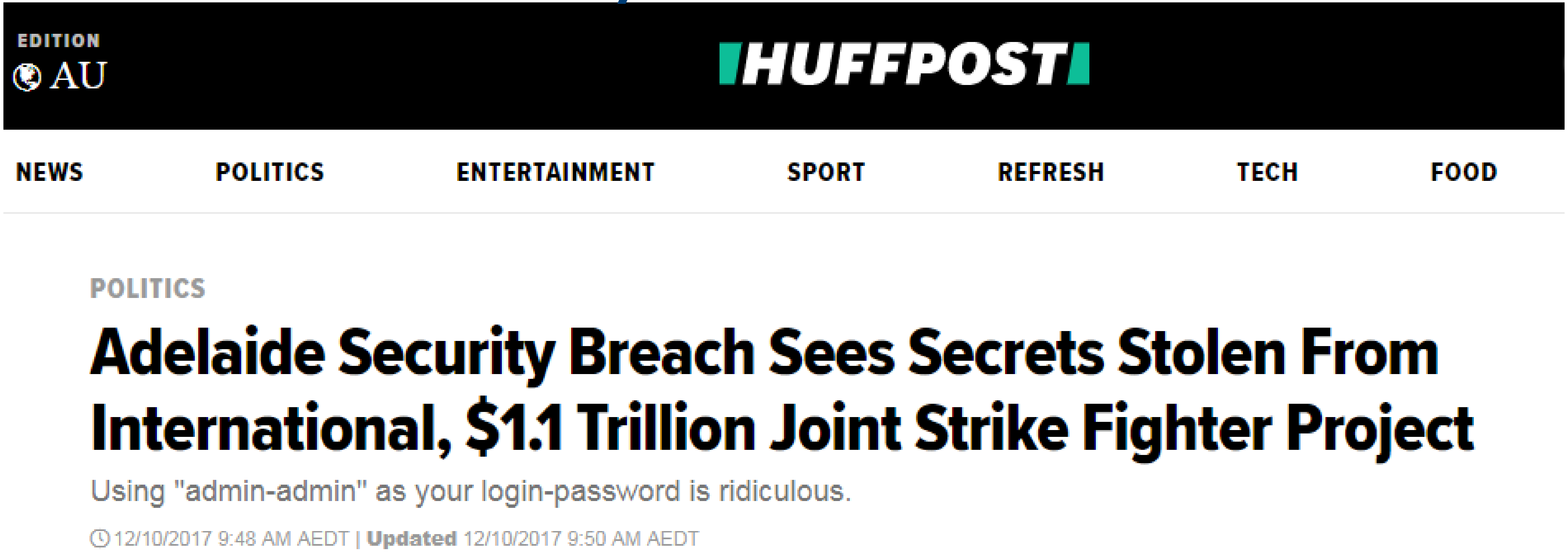
  ARTICLE 7. Accounting of Disclosures [1798.25 - 1798.29]
- *(Article 7 added by Stats. 1977, Ch. 709.)*
-

  1798.29.

What constitute protected data?

- Other protected Data (HIPPA, PCI, CJIS, CELTS, GDPR, PHI, NERC, Gramm-Leach-Bailey Act, FERPA and others)
- Business sensitive information that can cause harm if exposed
- National Security or classified material
- Intellectual property
- CAD, Diagrams or design documents

What are employees doing with your data?



EDITION
AU

HUFFPOST

NEWS POLITICS ENTERTAINMENT SPORT REFRESH TECH FOOD

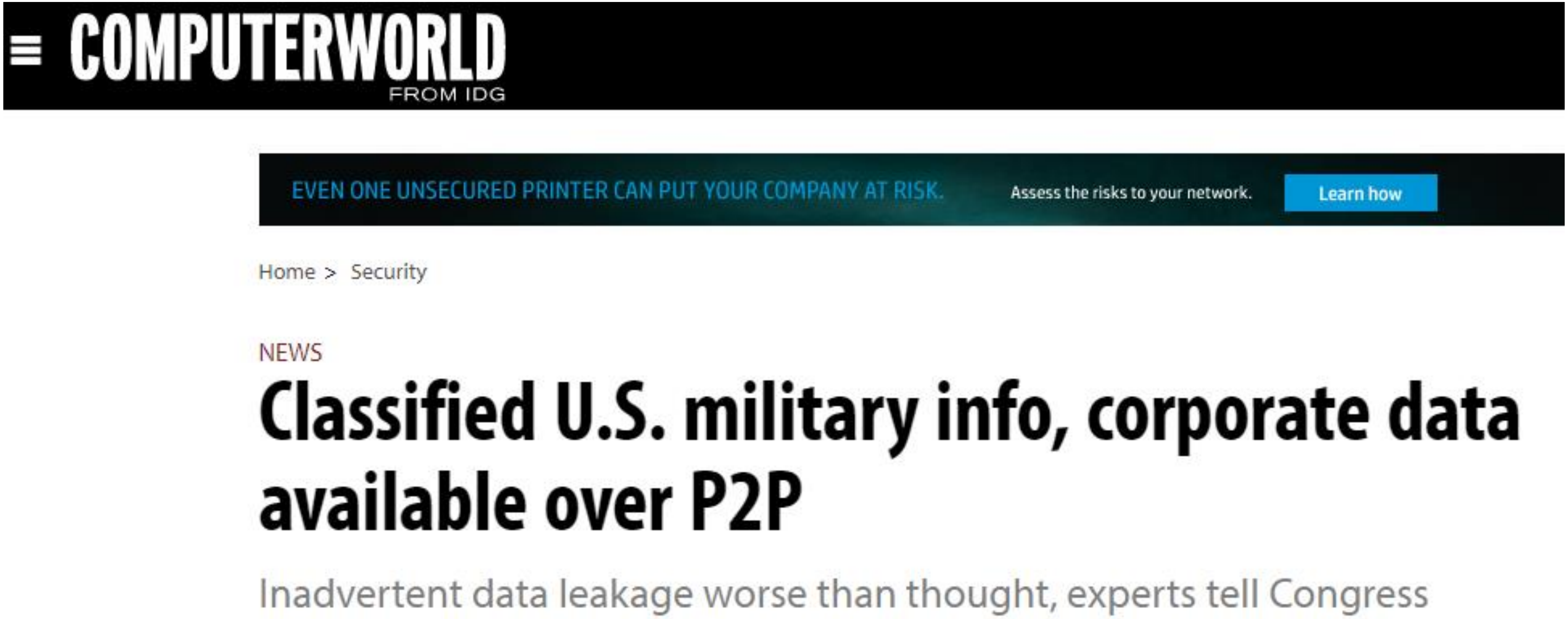
POLITICS

Adelaide Security Breach Sees Secrets Stolen From International, $1.1 Trillion Joint Strike Fighter Project

Using "admin-admin" as your login-password is ridiculous.

12/10/2017 9:48 AM AEDT | **Updated** 12/10/2017 9:50 AM AEDT

What are employees doing with your data?



COMPUTERWORLD
FROM IDG

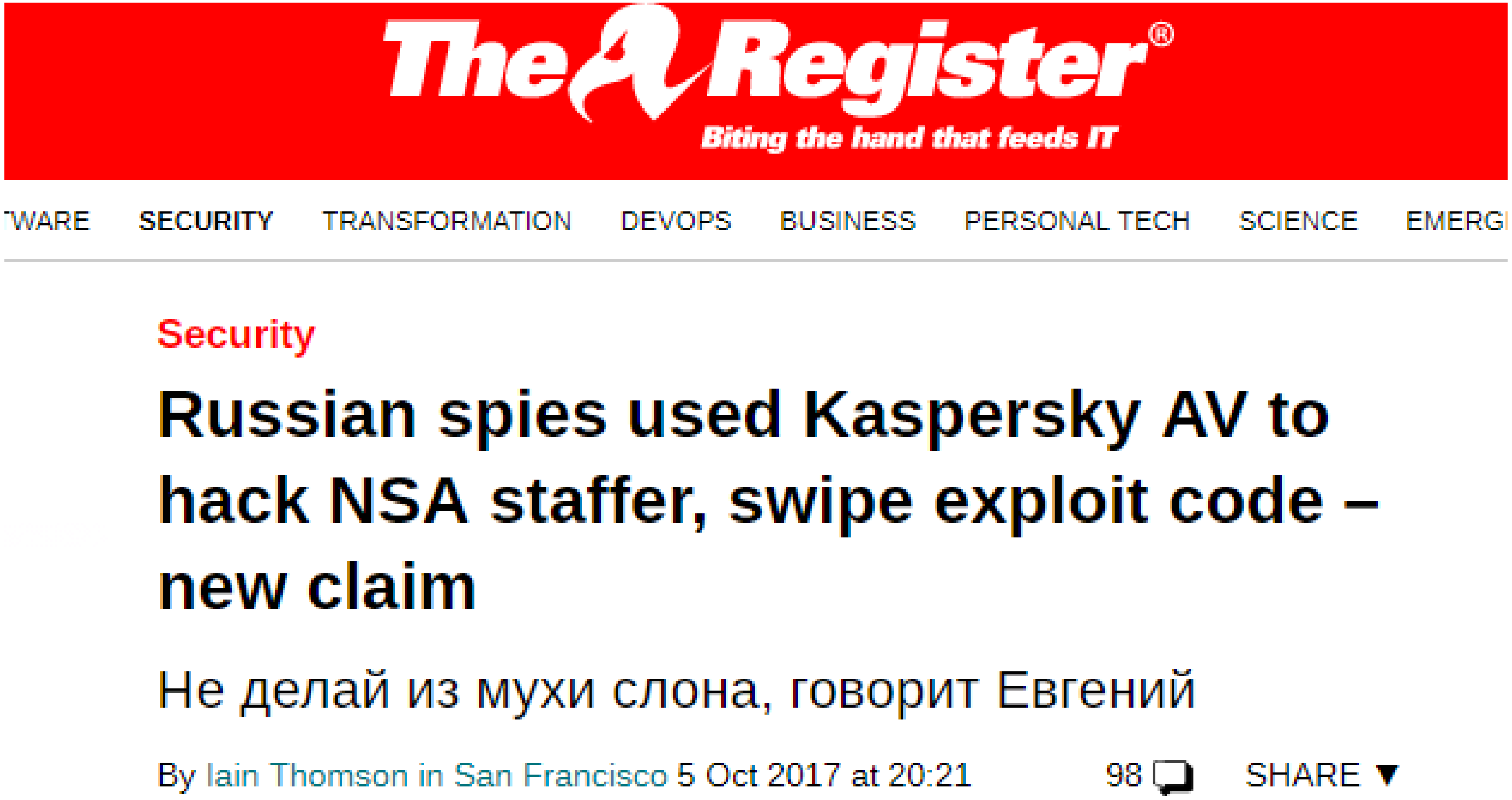
Home > Security

NEWS

Classified U.S. military info, corporate data available over P2P

Inadvertent data leakage worse than thought, experts tell Congress

What are employees doing with your data?



The Register®

Biting the hand that feeds IT

'WARE SECURITY TRANSFORMATION DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGI

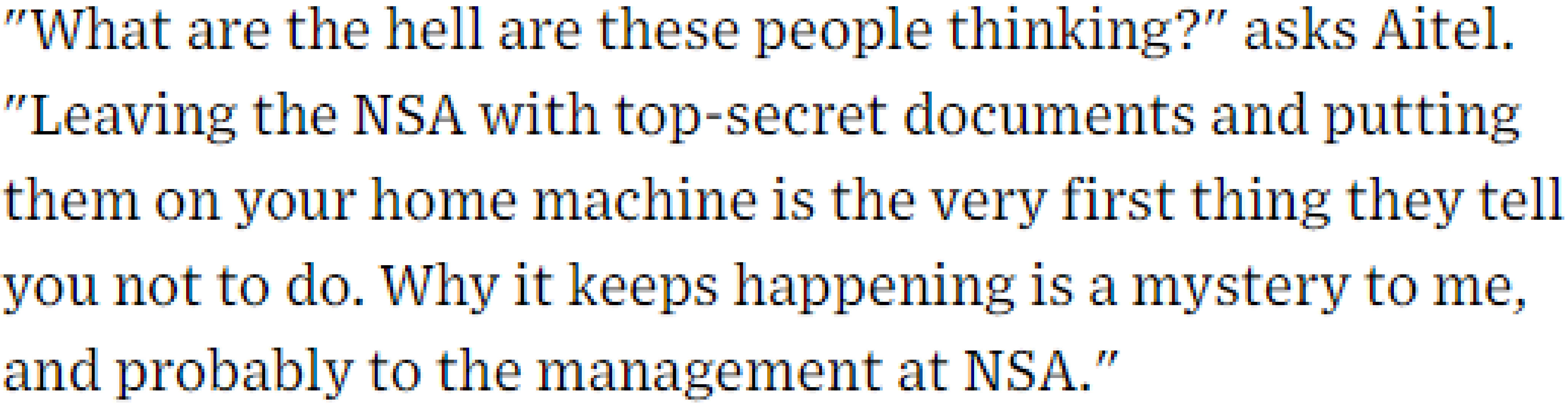
Security

Russian spies used Kaspersky AV to hack NSA staffer, swipe exploit code – new claim

Не делай из мухи слона, говорит Евгений

By Iain Thomson in San Francisco 5 Oct 2017 at 20:21 98 SHARE ▼

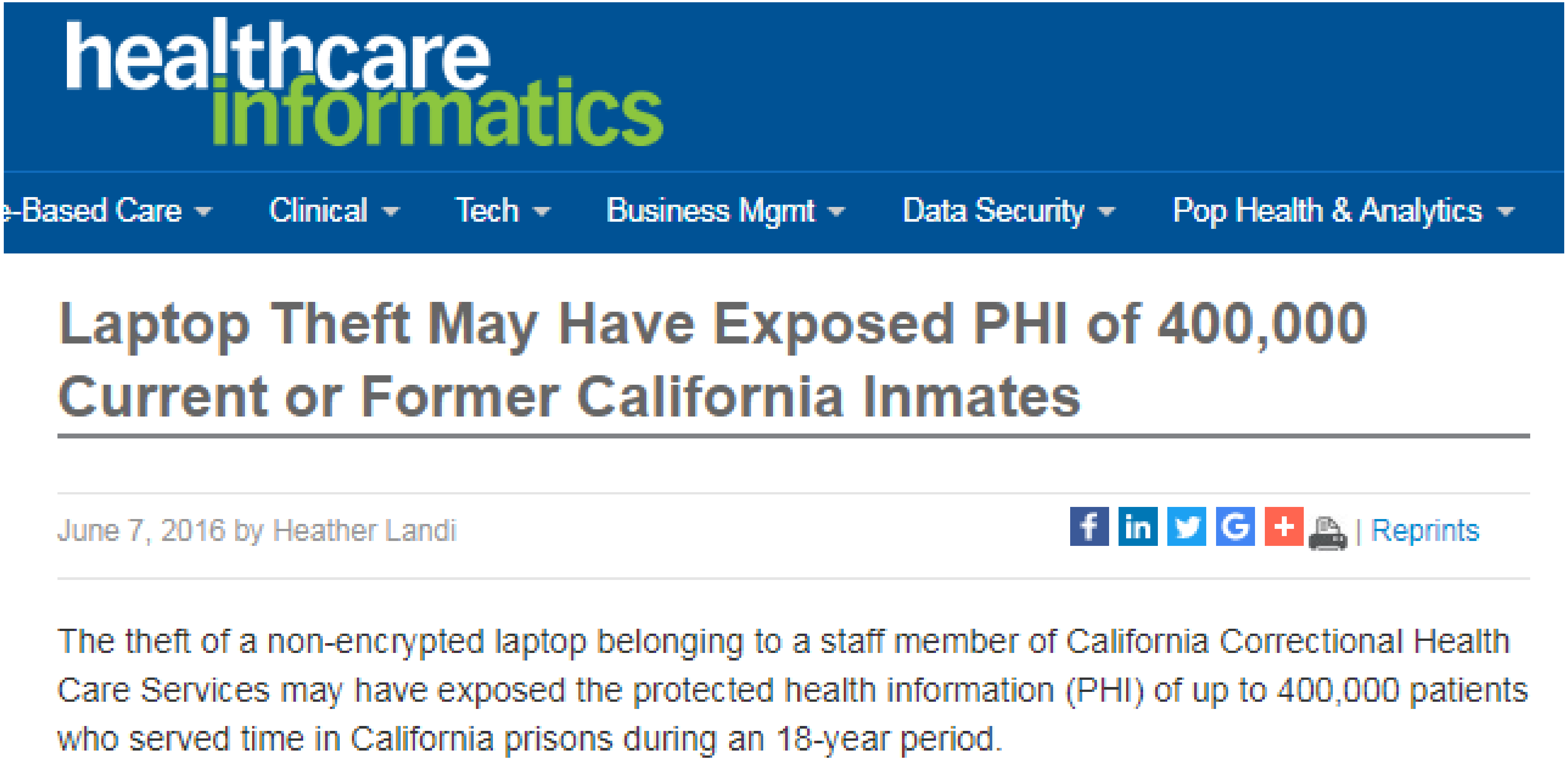
What are employees doing with your data?



"What are the hell are these people thinking?" asks Aitel. "Leaving the NSA with top-secret documents and putting them on your home machine is the very first thing they tell you not to do. Why it keeps happening is a mystery to me, and probably to the management at NSA."

ANDY GREENBERG, WIRED.COM 10.05.17

What are employees doing with your data?

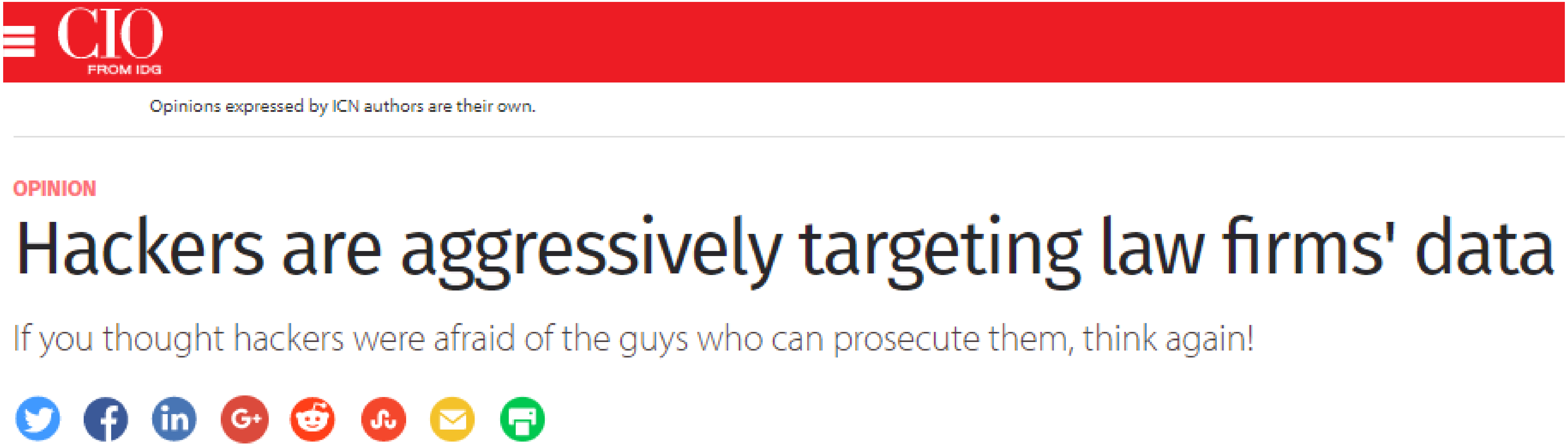


Laptop Theft May Have Exposed PHI of 400,000 Current or Former California Inmates

June 7, 2016 by Heather Landi

The theft of a non-encrypted laptop belonging to a staff member of California Correctional Health Care Services may have exposed the protected health information (PHI) of up to 400,000 patients who served time in California prisons during an 18-year period.

3rd Party risk?



CIO
FROM IDG

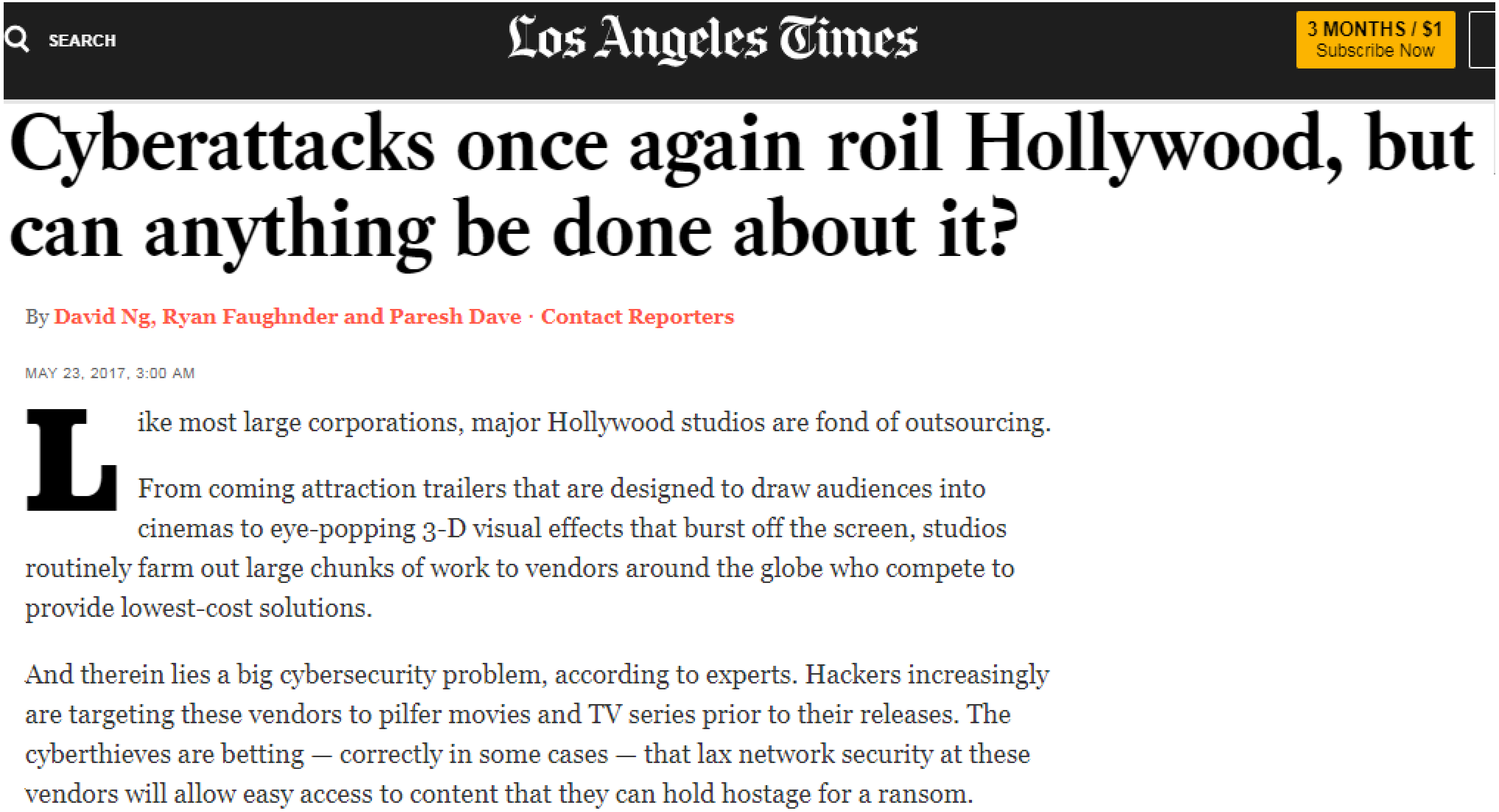
Opinions expressed by ICN authors are their own.

OPINION

Hackers are aggressively targeting law firms' data

If you thought hackers were afraid of the guys who can prosecute them, think again!

3rd Party risk?



Cyberattacks once again roil Hollywood, but can anything be done about it?

By David Ng, Ryan Faughnder and Paresh Dave · Contact Reporters

MAY 23, 2017, 3:00 AM

Like most large corporations, major Hollywood studios are fond of outsourcing.

From coming attraction trailers that are designed to draw audiences into cinemas to eye-popping 3-D visual effects that burst off the screen, studios routinely farm out large chunks of work to vendors around the globe who compete to provide lowest-cost solutions.

And therein lies a big cybersecurity problem, according to experts. Hackers increasingly are targeting these vendors to pilfer movies and TV series prior to their releases. The cyberthieves are betting — correctly in some cases — that lax network security at these vendors will allow easy access to content that they can hold hostage for a ransom.

6.7 Million Voter records

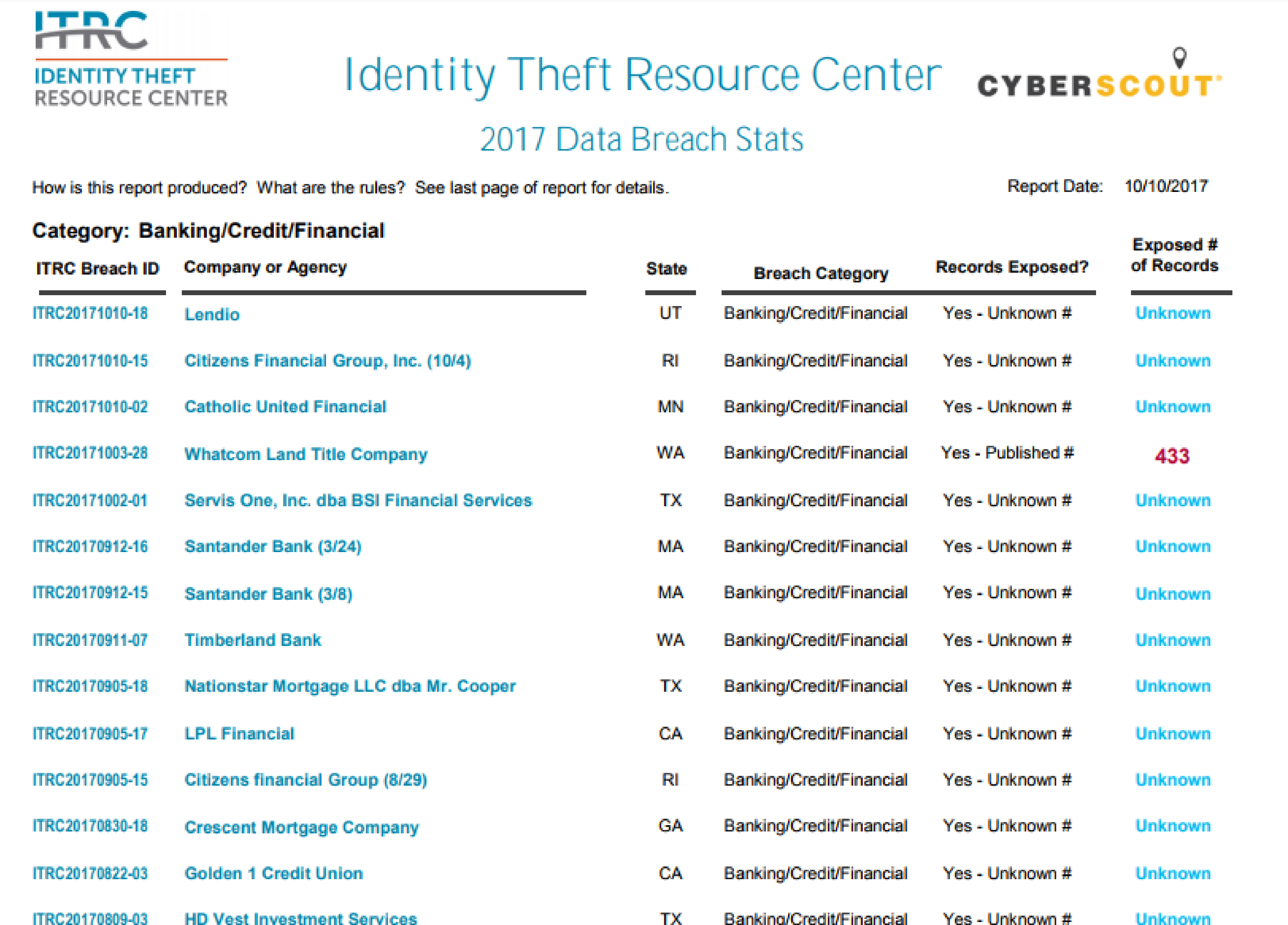
NEW YORK POST

Researcher discovers Georgia voter database exposed online

By Associated Press

June 15, 2017 | 2:41am

Do we even know where our data lives?



IDENTITY THEFT RESOURCE CENTER

Identity Theft Resource Center

CYBERSCOUT

2017 Data Breach Stats

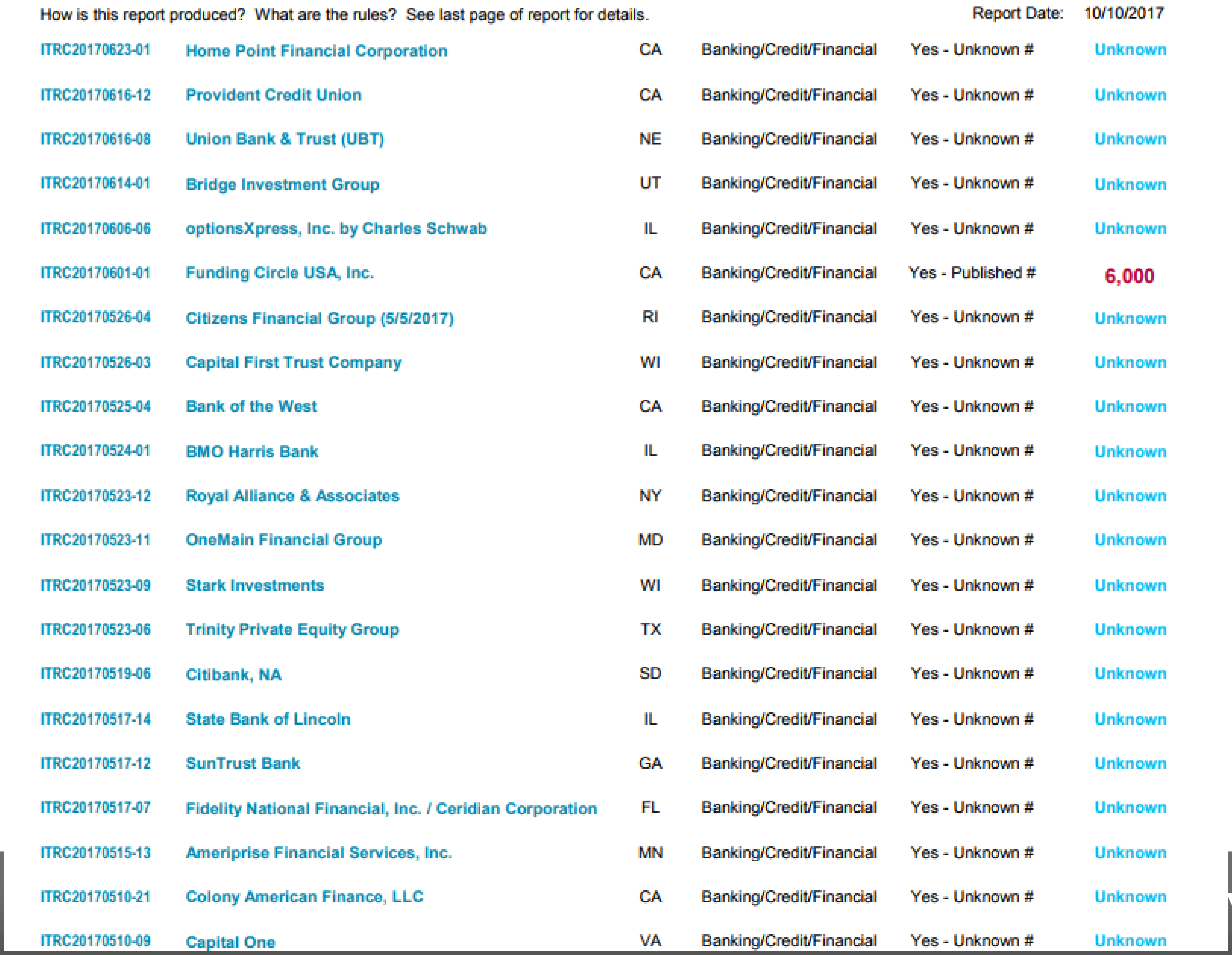
How is this report produced? What are the rules? See last page of report for details.

Report Date: 10/10/2017

Category: Banking/Credit/Financial

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20171010-18	Lendio	UT	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20171010-15	Citizens Financial Group, Inc. (10/4)	RI	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20171010-02	Catholic United Financial	MN	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20171003-28	Whatcom Land Title Company	WA	Banking/Credit/Financial	Yes - Published #	433
ITRC20171002-01	Servis One, Inc. dba BSI Financial Services	TX	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170912-16	Santander Bank (3/24)	MA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170912-15	Santander Bank (3/8)	MA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170911-07	Timberland Bank	WA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170905-18	Nationstar Mortgage LLC dba Mr. Cooper	TX	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170905-17	LPL Financial	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170905-15	Citizens financial Group (8/29)	RI	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170830-18	Crescent Mortgage Company	GA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170822-03	Golden 1 Credit Union	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170809-03	HD Vest Investment Services	TX	Banking/Credit/Financial	Yes - Unknown #	Unknown

Do we even know where our data lives?

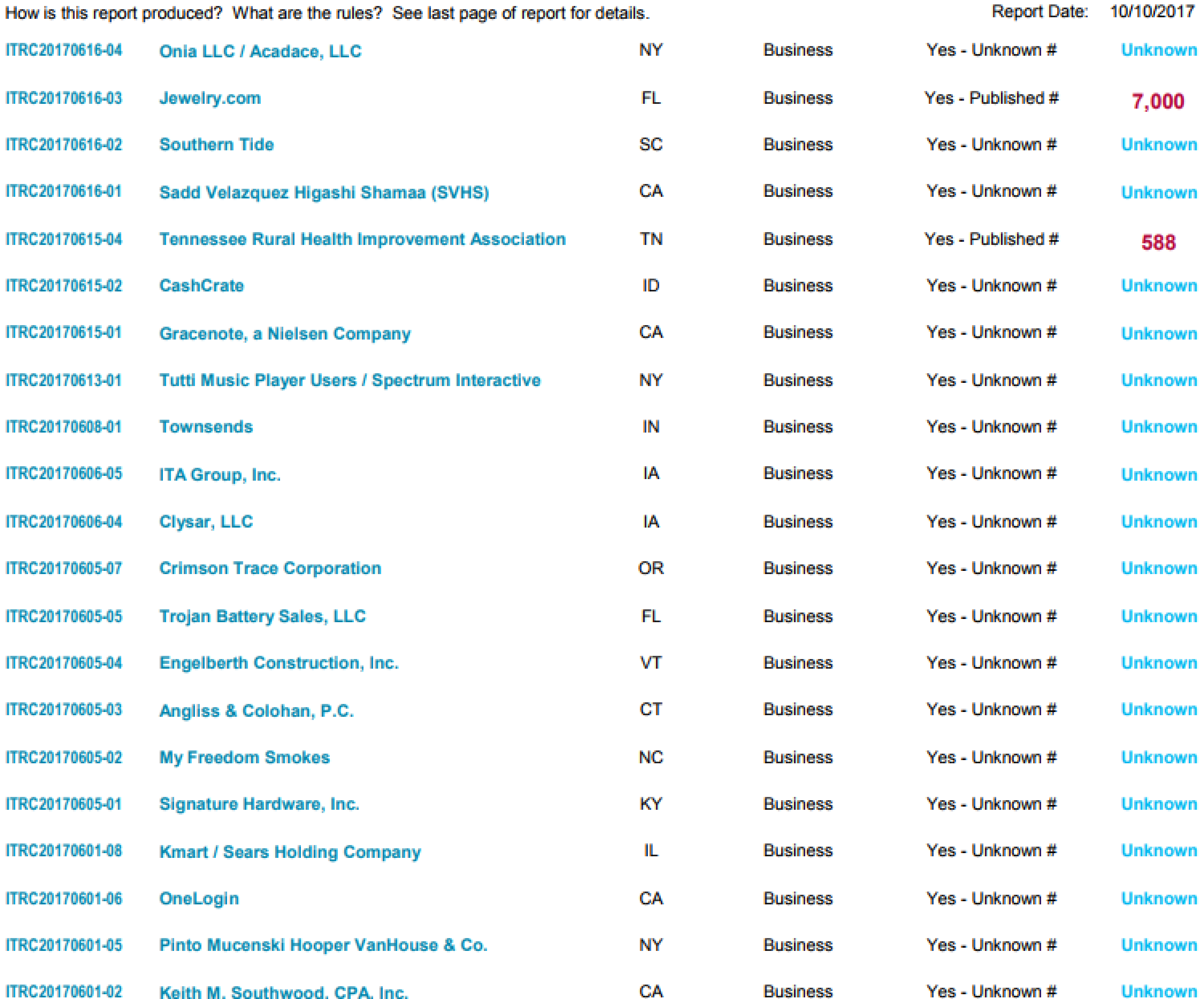


How is this report produced? What are the rules? See last page of report for details.

Report Date: 10/10/2017

ITRC20170623-01	Home Point Financial Corporation	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170616-12	Provident Credit Union	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170616-08	Union Bank & Trust (UBT)	NE	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170614-01	Bridge Investment Group	UT	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170606-06	optionsXpress, Inc. by Charles Schwab	IL	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170601-01	Funding Circle USA, Inc.	CA	Banking/Credit/Financial	Yes - Published #	6,000
ITRC20170526-04	Citizens Financial Group (5/5/2017)	RI	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170526-03	Capital First Trust Company	WI	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170525-04	Bank of the West	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170524-01	BMO Harris Bank	IL	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170523-12	Royal Alliance & Associates	NY	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170523-11	OneMain Financial Group	MD	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170523-09	Stark Investments	WI	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170523-06	Trinity Private Equity Group	TX	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170519-06	Citibank, NA	SD	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170517-14	State Bank of Lincoln	IL	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170517-12	SunTrust Bank	GA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170517-07	Fidelity National Financial, Inc. / Ceridian Corporation	FL	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170515-13	Ameriprise Financial Services, Inc.	MN	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170510-21	Colony American Finance, LLC	CA	Banking/Credit/Financial	Yes - Unknown #	Unknown
ITRC20170510-09	Capital One	VA	Banking/Credit/Financial	Yes - Unknown #	Unknown

Do we even know where our data lives?



How is this report produced? What are the rules? See last page of report for details.

Report Date: 10/10/2017

ITRC20170616-04	Onia LLC / Acadace, LLC	NY	Business	Yes - Unknown #	Unknown
ITRC20170616-03	Jewelry.com	FL	Business	Yes - Published #	7,000
ITRC20170616-02	Southern Tide	SC	Business	Yes - Unknown #	Unknown
ITRC20170616-01	Sadd Velazquez Higashi Shamaa (SVHS)	CA	Business	Yes - Unknown #	Unknown
ITRC20170615-04	Tennessee Rural Health Improvement Association	TN	Business	Yes - Published #	588
ITRC20170615-02	CashCrate	ID	Business	Yes - Unknown #	Unknown
ITRC20170615-01	Gracenote, a Nielsen Company	CA	Business	Yes - Unknown #	Unknown
ITRC20170613-01	Tutti Music Player Users / Spectrum Interactive	NY	Business	Yes - Unknown #	Unknown
ITRC20170608-01	Townsends	IN	Business	Yes - Unknown #	Unknown
ITRC20170606-05	ITA Group, Inc.	IA	Business	Yes - Unknown #	Unknown
ITRC20170606-04	Clysar, LLC	IA	Business	Yes - Unknown #	Unknown
ITRC20170605-07	Crimson Trace Corporation	OR	Business	Yes - Unknown #	Unknown
ITRC20170605-05	Trojan Battery Sales, LLC	FL	Business	Yes - Unknown #	Unknown
ITRC20170605-04	Engelberth Construction, Inc.	VT	Business	Yes - Unknown #	Unknown
ITRC20170605-03	Angliss & Colohan, P.C.	CT	Business	Yes - Unknown #	Unknown
ITRC20170605-02	My Freedom Smokes	NC	Business	Yes - Unknown #	Unknown
ITRC20170605-01	Signature Hardware, Inc.	KY	Business	Yes - Unknown #	Unknown
ITRC20170601-08	Kmart / Sears Holding Company	IL	Business	Yes - Unknown #	Unknown
ITRC20170601-06	OneLogin	CA	Business	Yes - Unknown #	Unknown
ITRC20170601-05	Pinto Mucenski Hooper VanHouse & Co.	NY	Business	Yes - Unknown #	Unknown
ITRC20170601-02	Keith M. Southwood, CPA, Inc.	CA	Business	Yes - Unknown #	Unknown

Do we even know where our data lives?

UNKNOWN

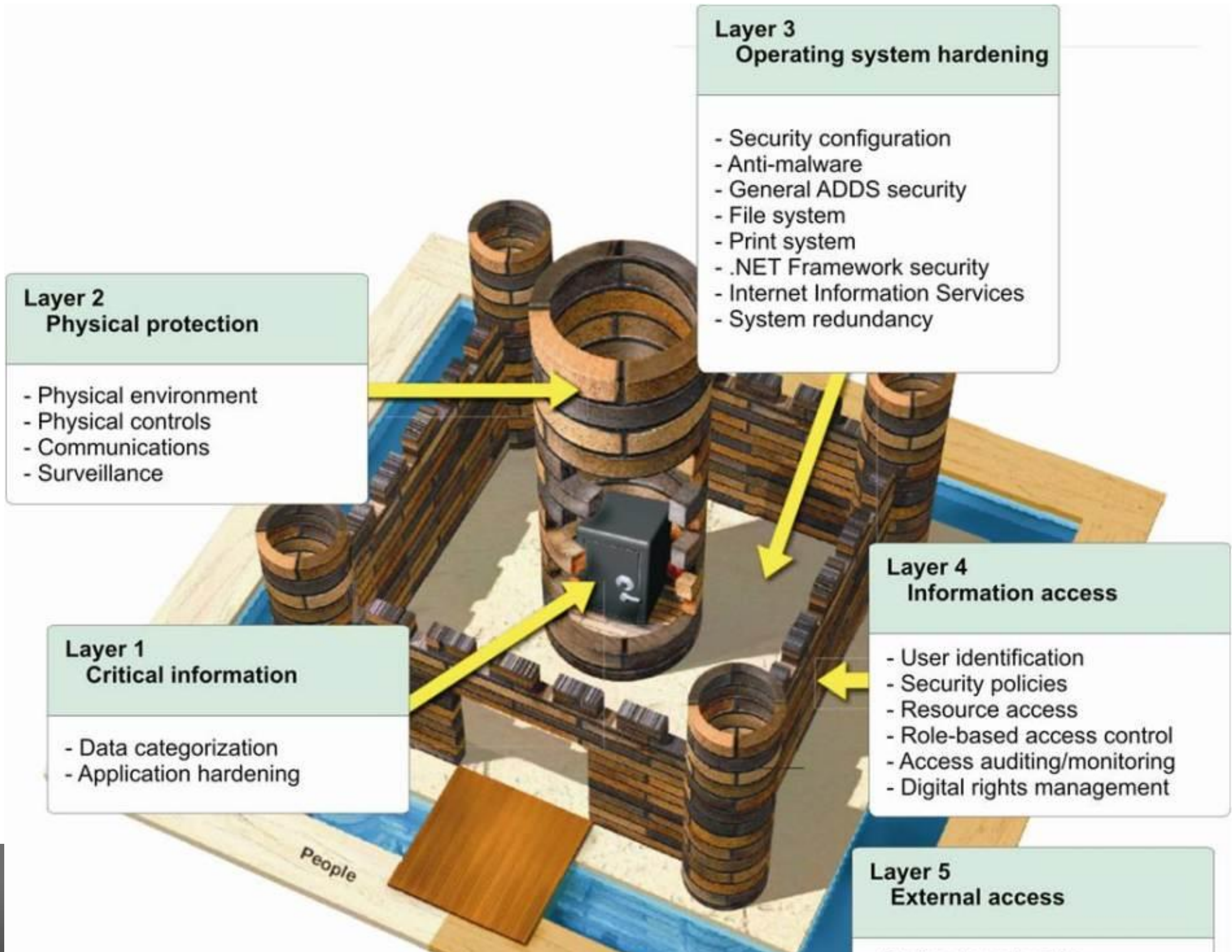
What do they have in common

- They all have:
  - – Firewalls
  - – Antivirus
  - – They Patch (at least some systems)
  - – They train their employees
  - – They don’t know where their data lives
  - – They lack the capability to determine what data was lost

What do they have in common

Did they lose sight of what are they supposed to protect?

Don’t get stuck in the how and forget why



Layer 3
Operating system hardening

- Security configuration
- Anti-malware
- General ADDS security
- File system
- Print system
- .NET Framework security
- Internet Information Services
- System redundancy

Layer 2
Physical protection

- Physical environment
- Physical controls
- Communications
- Surveillance

Layer 4
Information access

- User identification
- Security policies
- Resource access
- Role-based access control
- Access auditing/monitoring
- Digital rights management

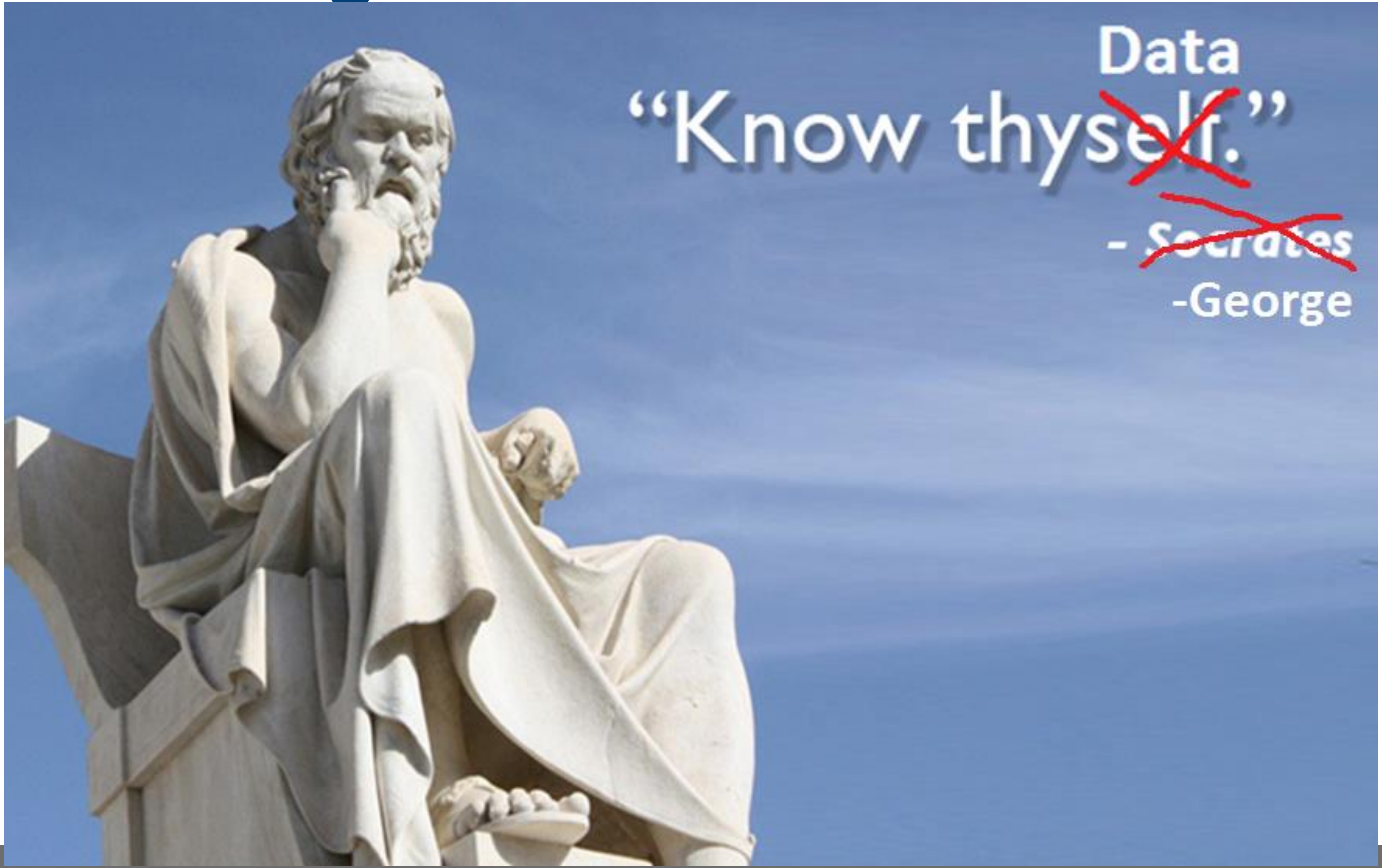
Layer 1
Critical information

- Data categorization
- Application hardening

Layer 5
External access

Can anyone protect this?

George's 21st Critical Control



Enterprise Data Security Challenges

- We all know where data should be stored
- But most of us don't know where data is stored
- Security operates in a continuous incident response loop
- The business does not understand the impact of a data breach
- Cleanup is a massive undertaking

Data Protection

- Establish Sensitive data handling policy
  - Establish sensitivity classification
  - Create document templates
  - Create watermarks, labels and meta data standards
  - Identify employee roles and restrict access
  - Update and enforce your data retention policies
    - You can’t lose what you don’t save

Data Protection

- Establish Data Safe Zones
  - Encrypt data at rest on servers and endpoints
  - Audit access, changes and deletion
  - Deploy user behavior analytics systems
    - Monitor spikes in data access, changes or deletion
    - Create normal baseline and alert on anomalies
  - Backup and test your disaster recovery plans
  - Enable frequent shadow copy / snapshots
  - Enforce end to end encryption

Data Protection

- Create Protected enclaves
  - Inspect encrypted communications to and from your secure enclaves
  - Create choke points to deploy your monitoring systems
  - Restrict communication and only allow required ports and protocols between your users and your secure enterprise applications
  - Deploy Web Application Firewalls to protect your public facing and internal applications

Data Protection

- **Review legacy data**
  - – Automatic discovery and classification of stored data
    - Include network shares and email
    - Desktops
    - Laptops
    - Mobile devices
    - Servers
    - Enterprise applications
    - Don’t forget the Cloud

Data Protection

- Engage your business
  - IT and Security are not the data custodians
  - Each business unit that generates data needs a Data Champion
  - Review how each business unit generates sensitive data
    - Most data is redundant and not needed
    - You often encounter duplicate records, reports and orphan files
    - Change risky business processes
    - Enforce your record retention policies

Data Protection

- Manage Data Life Cycle
  - – Beware of unauthorized Cloud Sync apps
  - – Deploy Automated DLP identification and blocking systems
  - – Create Automated policies to respond and contain protected data
    - Automatically move data to protected enclave
    - Create work flows to your department Data Champion
    - Change user behavior
    - Correct broken business processes

Data Protection

- Offensive Data Security
  - Canary in the mine / Honey Files
    - Create dummy files with important name
    - Embed trackers, beacons
    - Log and alert on access
  - Black holes
  - Counter intelligence campaign
    - Internal and external
- 3rd party access virtual Air gap

Data Protection

- Offensive Data Security
  - Canary in the mine / Honey Files
    - Create dummy files with important name
    - Embed trackers, beacons
    - Log and alert on access
  - Black holes
    - Large files to trigger behavior and file transfer alerts
    - Consume the attackers disk space
    - Slow the attacker down
  - Counter intelligence campaign
    - Advertise fake projects and fake staff, monitor these keywords heavily

Data Protection

- Application security
  - Who manages your encryption keys?
  - An application vulnerability+ application managed encryption keys = breach
  - Database encryption does not protect from employees running reports containing sensitive data
  - Hash+Salt your passwords
  - If possible encrypt data through it's entire lifecycle (including reports)
  - Build systems to allow revoking the encryption certificates after it leaves your organization

Data Protection

- "Air Gap" your vendors
- Change all service accounts and built in logins
- Enable Dual factor authentication for staff, vendors and system administrators
- Isolate your test, development and training environment from production systems
- Review user access rights annually and require reauthorization for sensitive systems.

Data Protection

– You can’t lose what you don’t have

Remember, Everything you save can and will be used against you in the event of a breach

QUESTIONS?

For a copy of this presentation, email me at gkhalil@Riversideca.gov
www.linkedin.com/in/george-khalil-Riverside