Cyber Challenges for Industry. Keeping the OT-IT running in the time of Cyber weaponization. Welcome to the Circus!

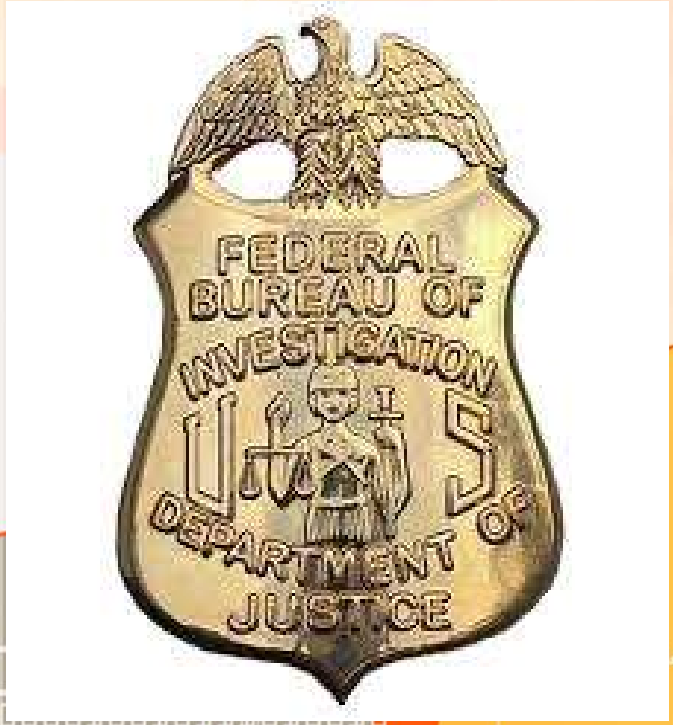
Donald R. Codling

Retired FBI Unit Chief, FBI Cyber Division

CISO-CPO advisor to multiple companies.

Don@codlinggroup.com

Mobile number +1-703-232-9015



Topics we will touch on

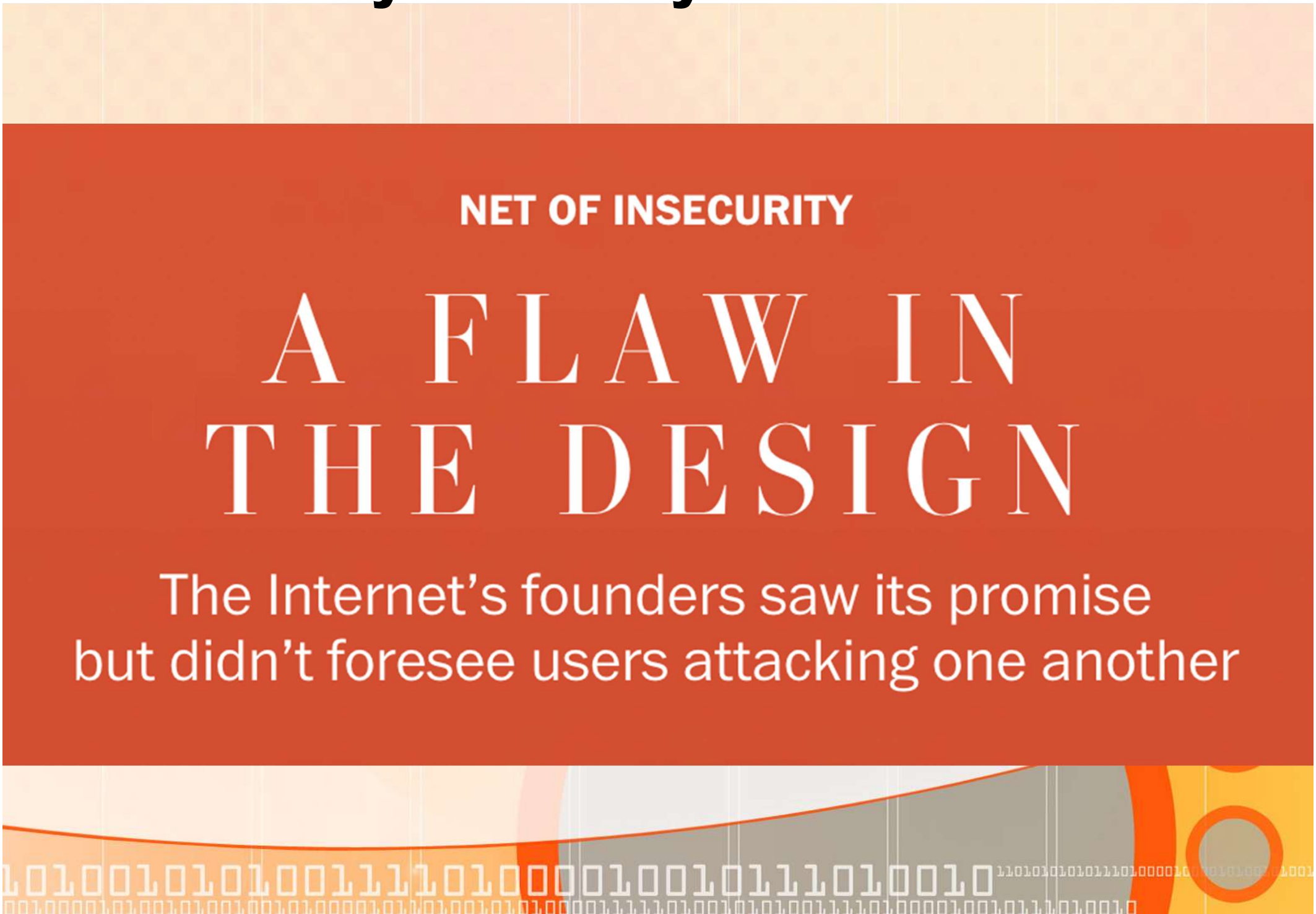
- *Cyber Weaponization is everywhere.*
- *Always ‘on’ IT and OT world—Maybe not?*
- *Challenges to ICS systems = Separate IT and OT systems networks with redundancy.*
- *Hacker Tools for fun and “profit”.*
- *Why BC/DR plans are so important.*
- *Vulnerability Awareness-CVE patching.*
- *3 copies of your CRITICAL DATA off your network – Secure Cloud backups.*

2023 off to a great start...NOT...

Has YOUR company done an Impact Assessment- what can you lose, then rebuild and start over again?

On the Internet, Nobody Knows You're a Dog

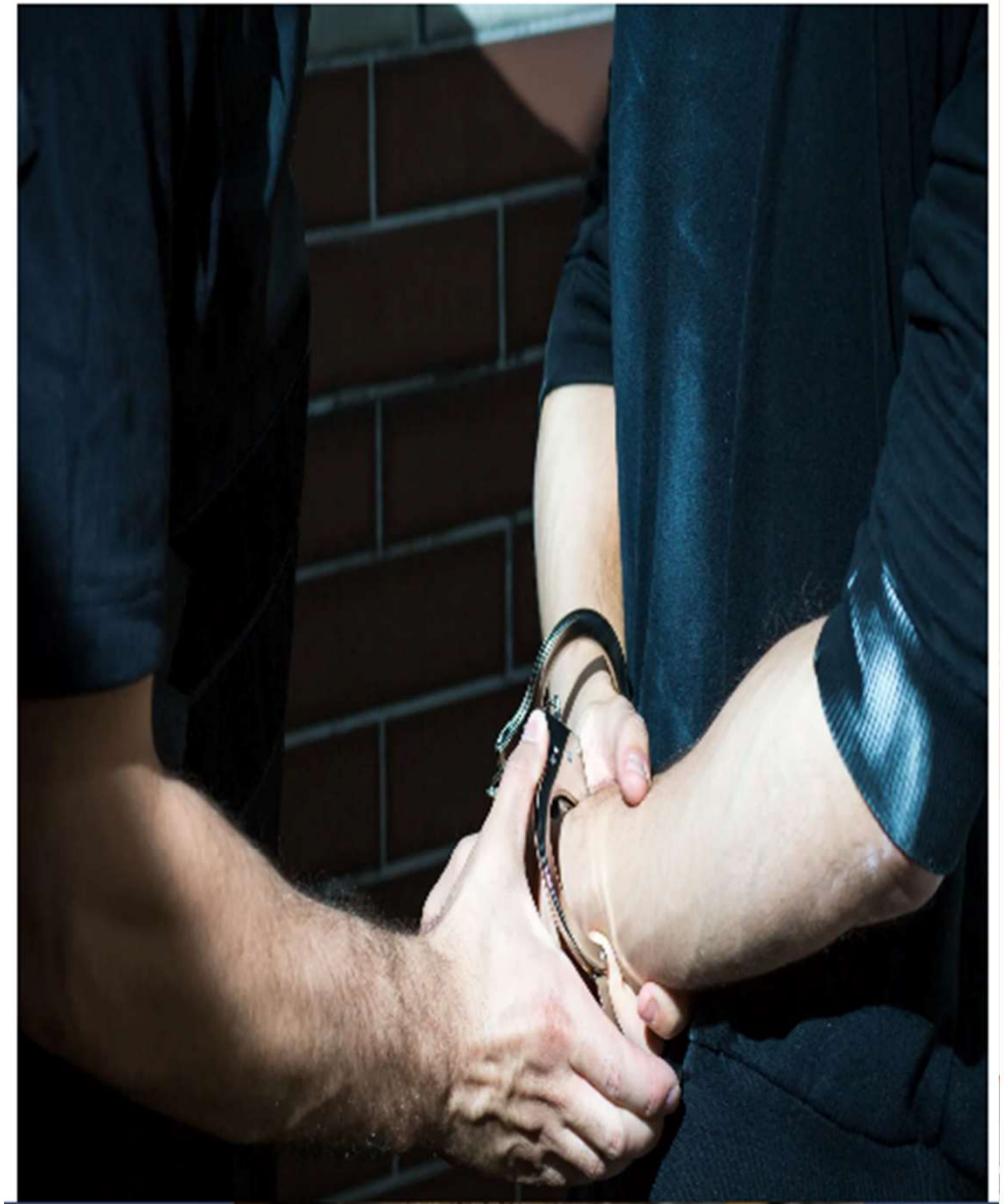
Internet sadly....Security was NEVER built in.



Bad guys-hacktivists are always looking for flaws

A Police App Exposed Secret Details About Raids and Suspects

SweepWizard, an app that law enforcement used to coordinate raids, left sensitive information about hundreds of police operations publicly accessible.



ODIN Intelligence website is defaced as hackers claim breach

Zack Whittaker

@zackwhittaker / 3:20 PM CST • January 15, 2023

Comment

Image Credits: ODIN Intelligence / YouTube

The website for ODIN Intelligence, a company that provides technology and tools for law enforcement and police departments, was defaced on Sunday.

Bottom Line- Low attacker Risk- High Reward

Never forget a vital part of Cyberspace….

HUMANS-

THE HARDEST PART OF ANY SYSTEM TO “PATCH” OR “UPDATE”.

Free public WiFi- No Thanks...ever

SALE

WIFI PINEAPPLE

$129.99

The leading rogue access point and WiFi pentest toolkit for close access operations. Passive and active attacks analyze vulnerable and misconfigured devices.

The WiFi Pineapple® NANO and TETRA are the 6th generation pentest platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 10 years of WiFi attack expertise.

WIFI PINEAPPLE

TETRA BASIC | NANO BASIC | ~~TETRA TACTICAL~~ | NANO TACTICAL

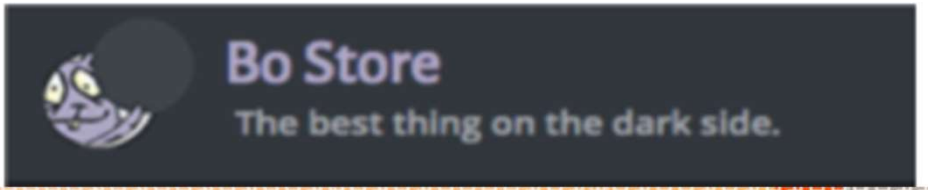
QTY

— 1 +

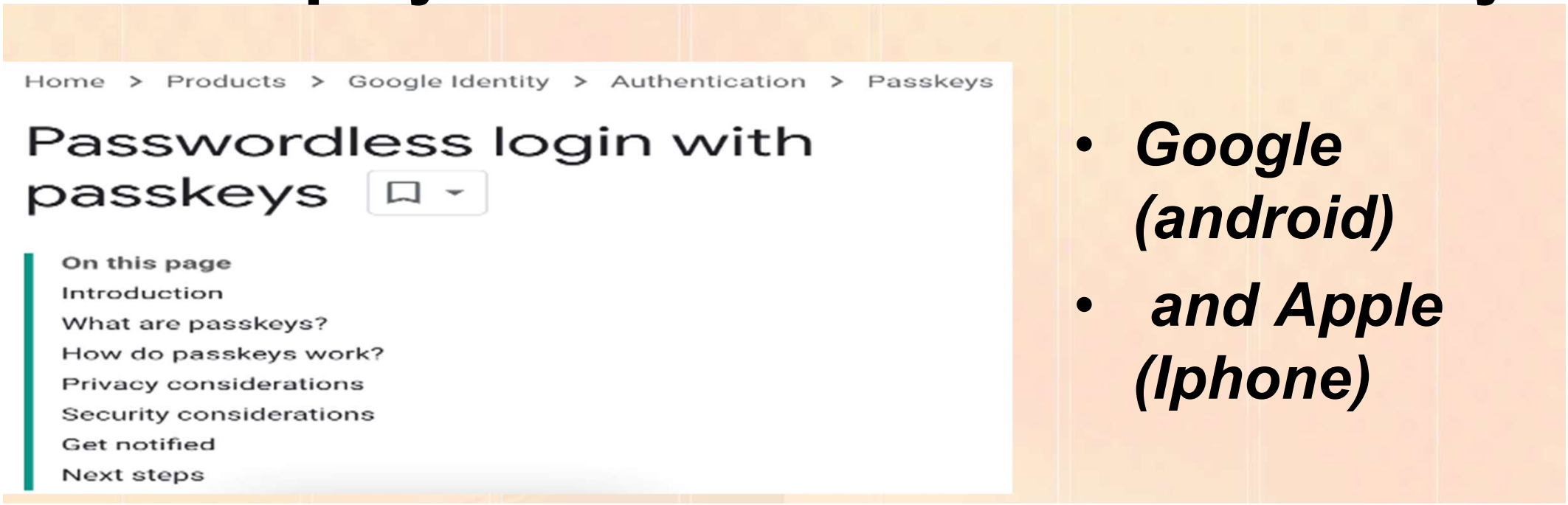
Prices for access as a service to "Networks" on the Dark Web Market as of 12/ 2022.

- ***Sandworm****-Russian-to launch "RansomBoggs" package- 1 "tool" -$5,000 USD unlimited use for 1 day.*
- *Russian Underground market-**MagBo-***
- *3000 websites-to include Power companies-city water systems as low as $5.00 to $1,000 per site for admin access.*

Access to approximately 3,000 breached websites has been discovered for sale on a Russian-speaking underground marketplace called MagBo. Access to some of the sites is selling for as low as 50 cents (USD).



After Company meltdown- NO PUBLIC WiFi -Passkeys



Sign in with passkeys on iPhone

Passkeys give you a simple and secure way to sign in without passwords by relying on Face ID (supported models) or Touch ID (supported models) to identify you when you sign in to supporting websites and apps.

Intro to passkeys

Based on industry standards for account authentication, passkeys are easier to use than passwords and far more secure.

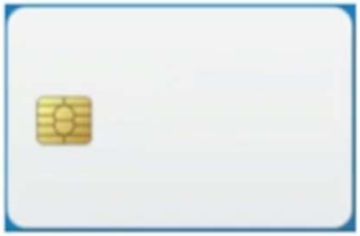
A passkey is a cryptographic entity that's not visible to you, and it's used in place of a password. A passkey consists of a *key pair*, which—compared to a password—profoundly improves security. One key is public, registered with the website or app you're using. The

The old fashioned way is becoming “new again” with hardware based Passkeys

Types of MFA

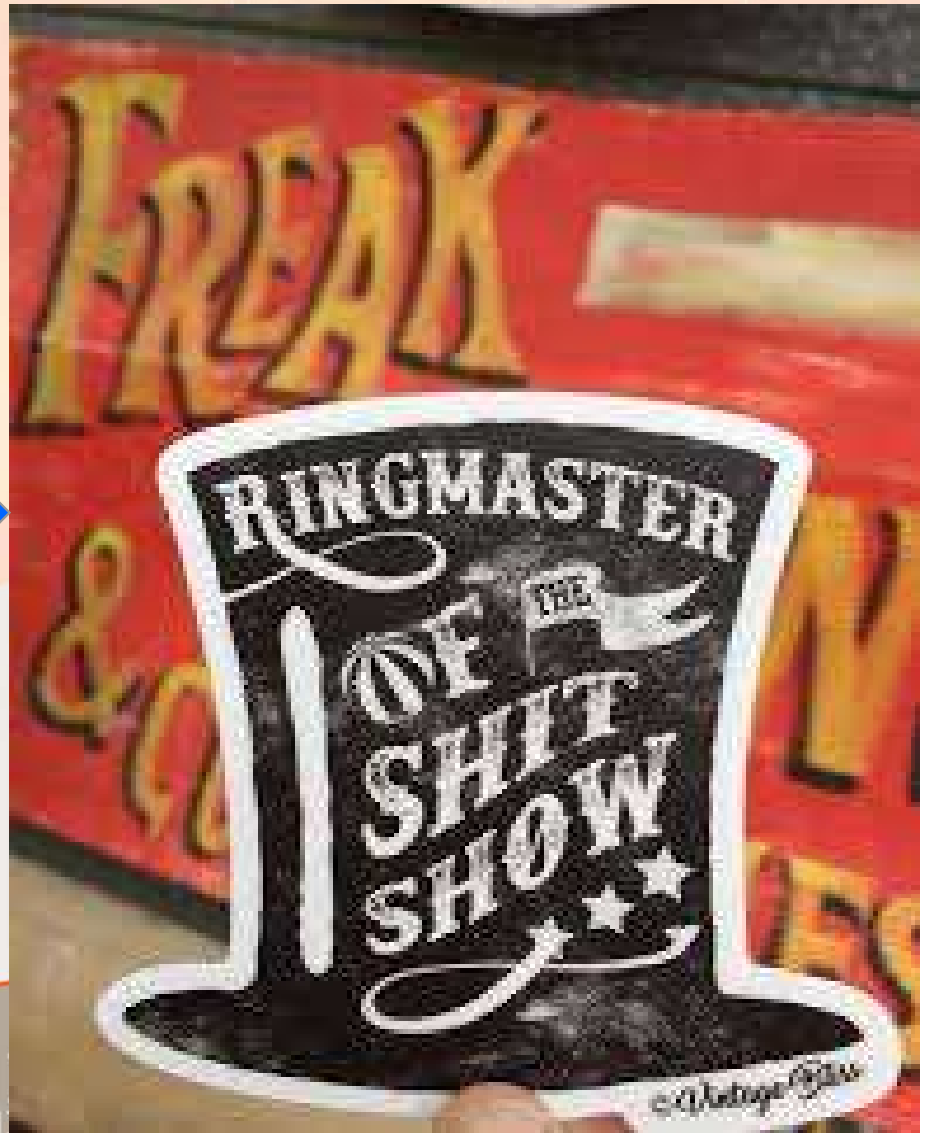
Token-Based MFA

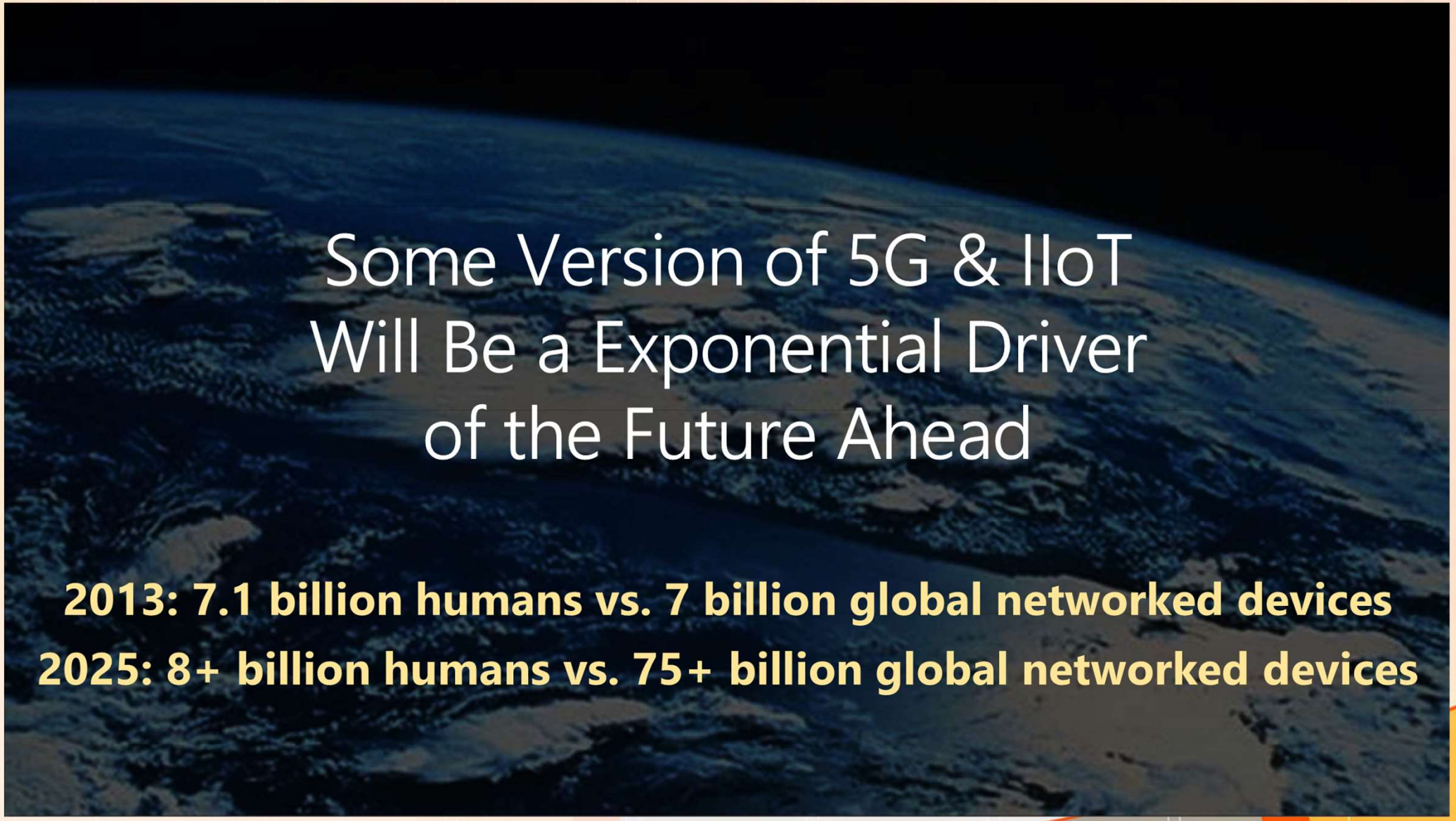
- Wired or wireless
- Smartcards
- USB-style tokens
- Credit-card style
- RFID cards
- FIDO keys
- Yubikeys



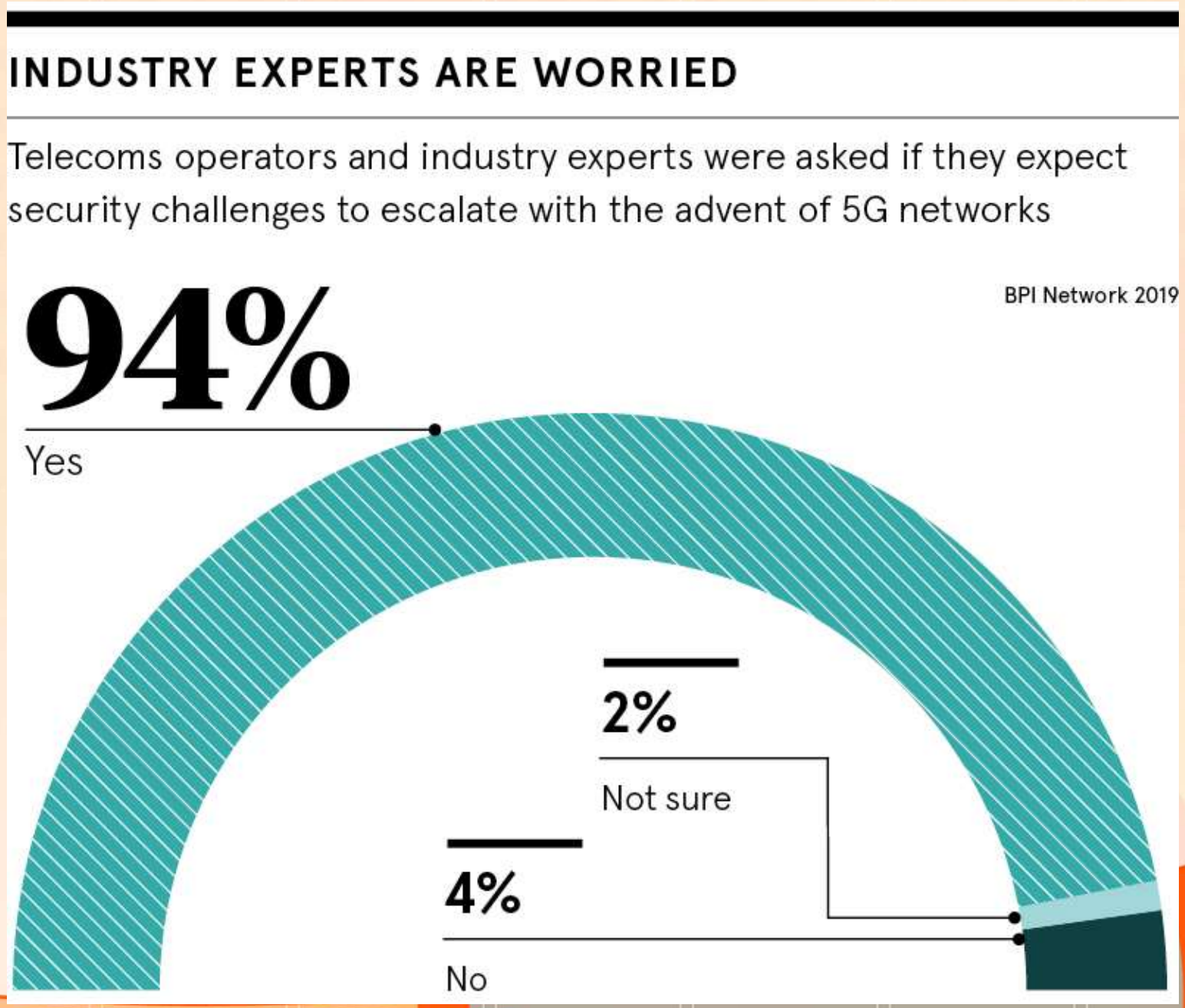
Unless Properly prepared-this inevitably happens…

Companies MUST remember the BASICS
-good Cyber Hygenie…Access Control and in todays world-secure cloud backups of settings…If FORGOTTEN…




Some Version of 5G & IIoT
Will Be a Exponential Driver
of the Future Ahead
2013: 7.1 billion humans vs. 7 billion global networked devices
2025: 8+ billion humans vs. 75+ billion global networked devices

More devices-More data-less room for error



Really Fast with LOTS of traffic

5G network and OT things can always break-right?

- *Like Canada discovered in July 2022 when the spine is severed-lots of 'stuff' stops working!*
- *More than 25% of the population was cut off for about 19 hours*

Soooo…What will 'data overload' look like?

How about NO Data??

Canada

Massive network outage in Canada hits homes, ATMs and 911 emergency lines

Rogers, which dominates mobile and internet market, says teams working to restore service amid widespread disruptions

Whats the difference- IT or OT?

- *IT (Information Technology)* ***controls data creation and flows****.*
- *Data transmission*
- *Information sharing*
- *Information gathering*
- *Hardware-software-peripherals*

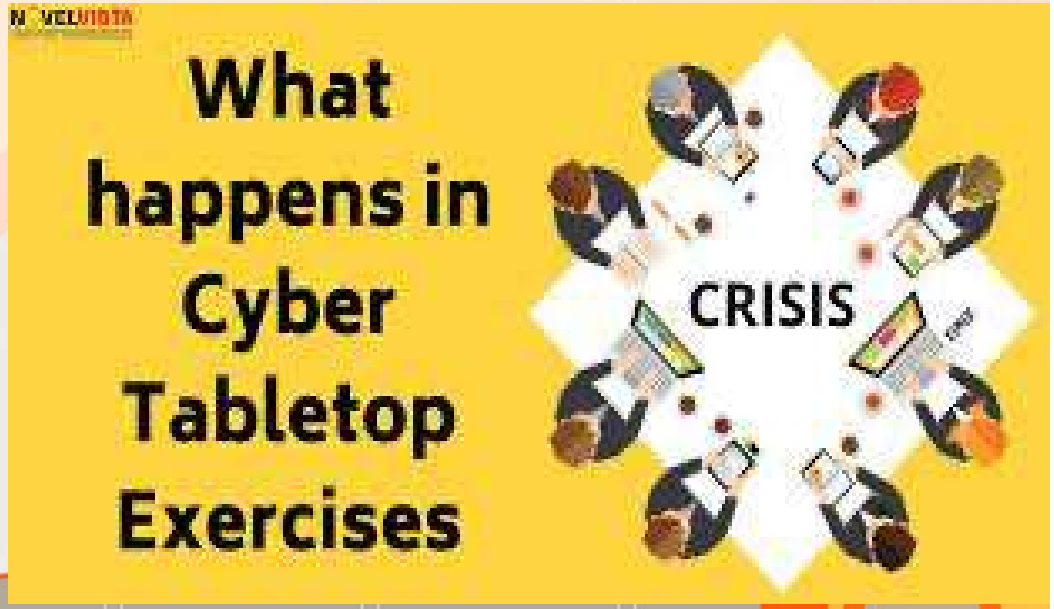
****Think Microsoft, Apple,*

- *OT (Operational Technology)* ***controls the physical world.***
- *Industrial Control Systems*
- *Machines that do things in the physical world like pump water, generate power.*

****Think Schneider Electric, Honeywell*

IT and OT cyber security –a matter of perspective

- *The most 'successful groups' know both simple and complex systems MUST work side by side.*
- *And they practice with table top exercises regularly to test when things BREAK!*
- *Where is that Business Continuity /Disaster Recovery plan again??*



The UGLY part of “IT”

OT-The soft underbelly of everything

RED ALERT | 5-MINUTE READ

Feds Uncover a 'Swiss Army Knife' for Hacking Industrial Systems

BY ANDY GREENBERG

The malware toolkit, known as Pipedream, is perhaps the most versatile tool ever made to target critical infrastructure like power grids and oil refineries.

PipeDream Anyone?

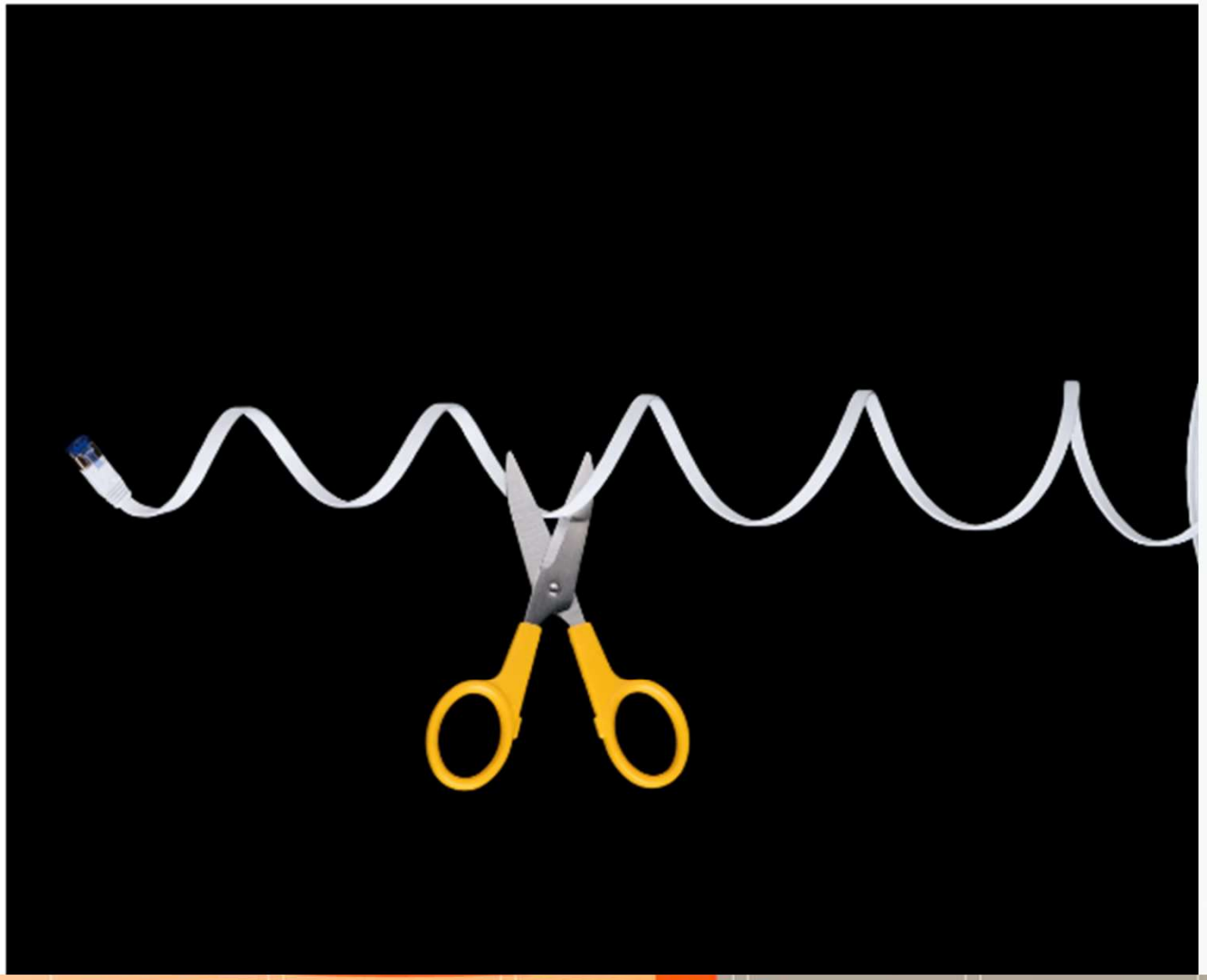
Feds Uncover a 'Swiss Army Knife' for Hacking Industrial Control Systems

The malware toolkit, known as Pipedream, is perhaps the most versatile tool ever made to target critical infrastructure like power grids and oil refineries.

April and July 2022

The Unsolved Mystery Attack on Internet Cables in Paris

As new details about the scope of the sabotage emerge, the perpetrators—and the reason for their vandalism—remain unknown.



6:16 AM · Apr 27, 2022

Wow, how did this happen?

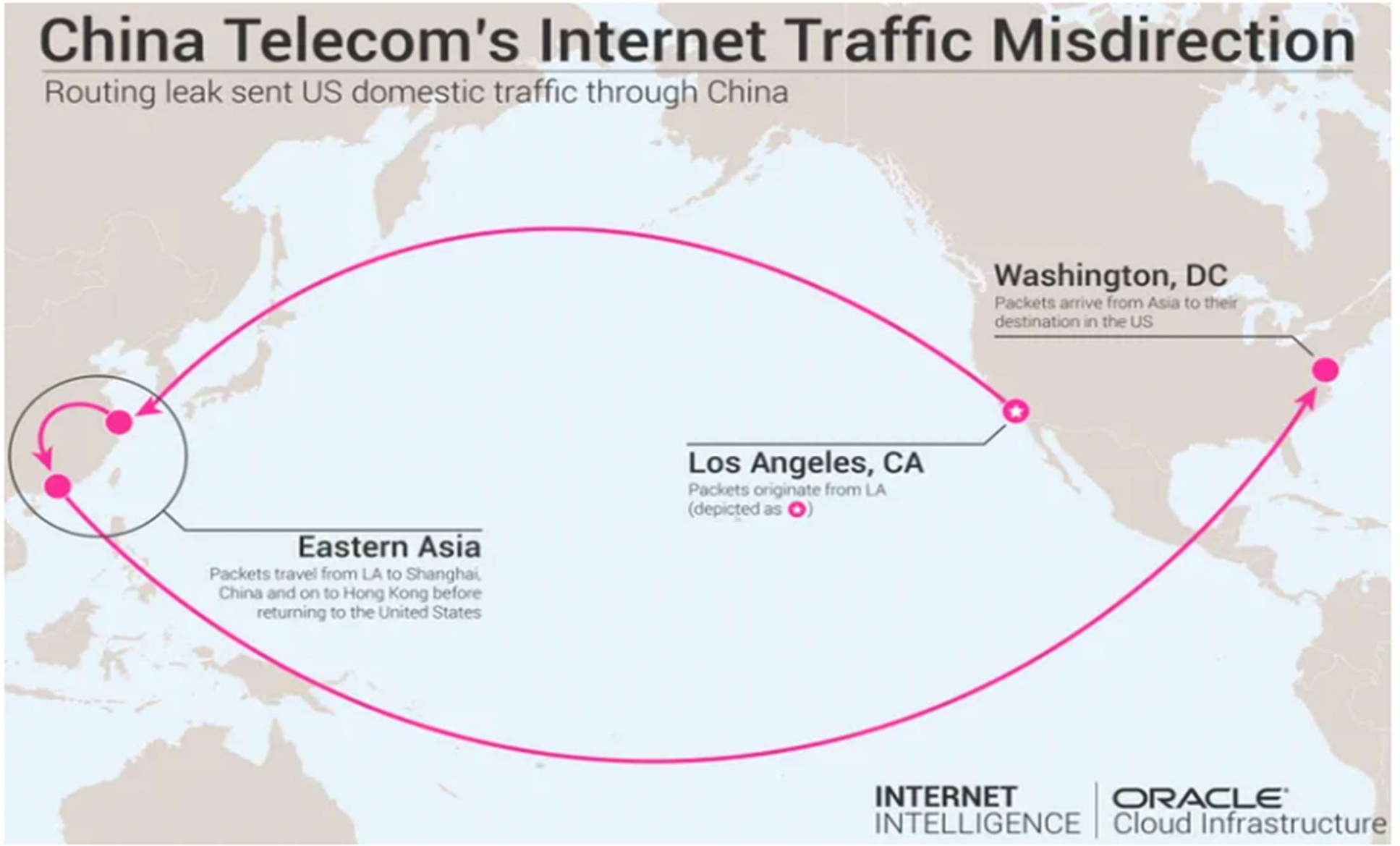


Image: Oracle Internet Intelligence

Not just America

THANKS, BGP. —

BGP event sends European mobile traffic through China Telecom for 2 hours

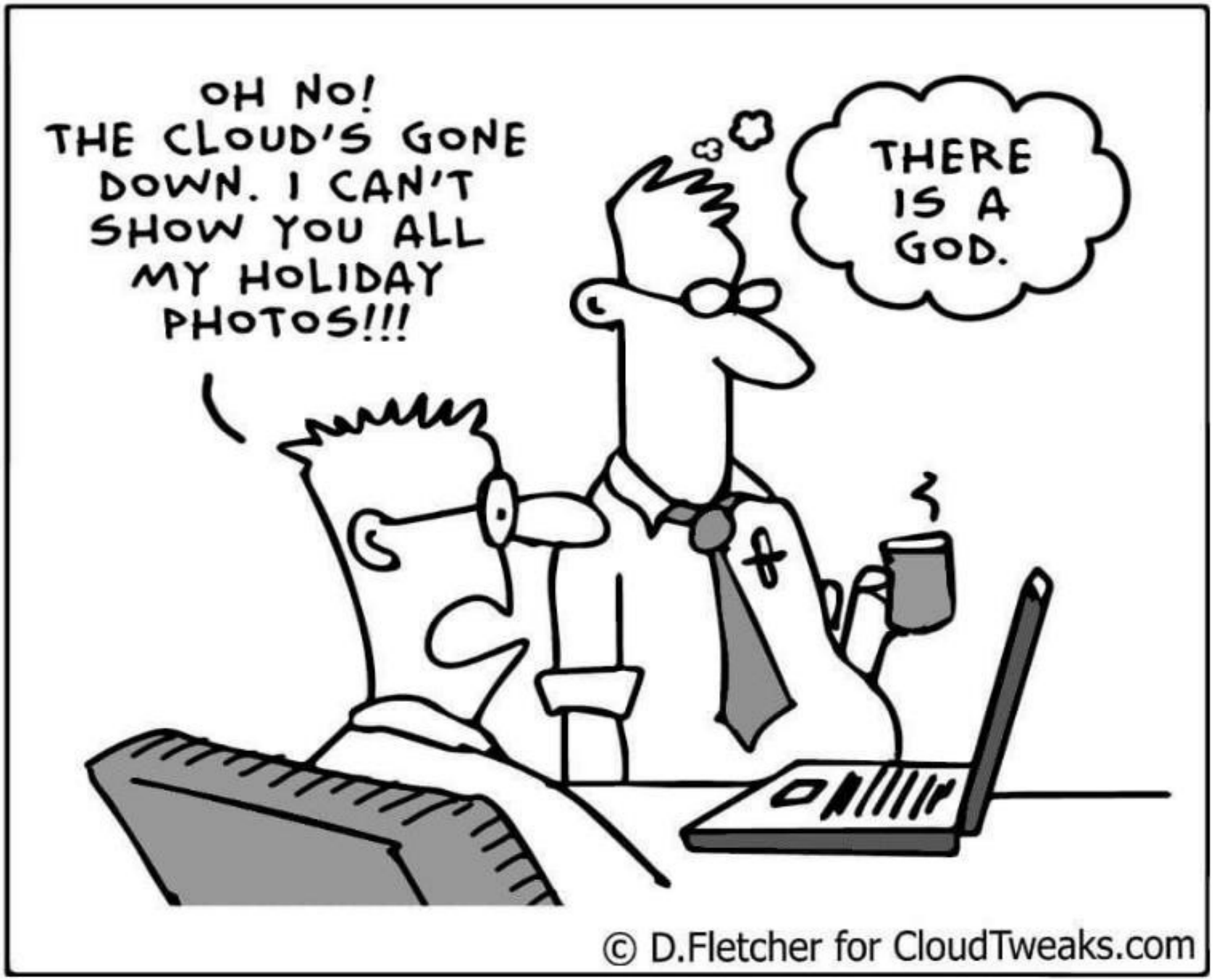
Improper leak to Chinese-government-owned telecom lasts up to two hours.

DAN GOODIN - 6/8/2019, 11:05 AM

The 11th Commandment... 3-2-1 rule

- *"Back up weekly- keep backups pure"*
- 3 copies in 2 formats and 1 copy offline!
- Encrypt data automatically? Yes please!
- Windows Automatic backups of ICS system settings to disk are NOT enough. Ransomware specifically looks for those files now.
- Must have-Paper copy of BC/DR plan for critical IRT people with Phone numbers

So lets talk about cloud storage



Cloud Backups-Critical settings

- **AWS, Azure or Oracle- all offer high security features & ransomware recovery.**
- **MSSP like ARMOR**
- **Encrypted Hard Drives- USB Thumb Drives MUST be physically removed and NOT accessible from the internet.**

- *File "STORAGE" is NOT the same as Data-Setting "BACKUP".*

Good free spots to get Cyber smarter…

- *Thecyberwire.com*
- *https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/scada*
- *www.KrebsonSecurity.com.*
- *Best Sunday reading….www.securethevillage.org*

SECURE THE VILLAGE

Cybersecurity News of the Week, January 22, 2023

A weekly aggregation of important cybersecurity and privacy news designed to educate, support, and advocate; helping you meet your data care challenges and responsibilities.

Where to find OT defense tips

- *ENISA, www.dragos.com/OT-CERT and Tenable.OT subsection on ICS- all EXCELLENT sources.*

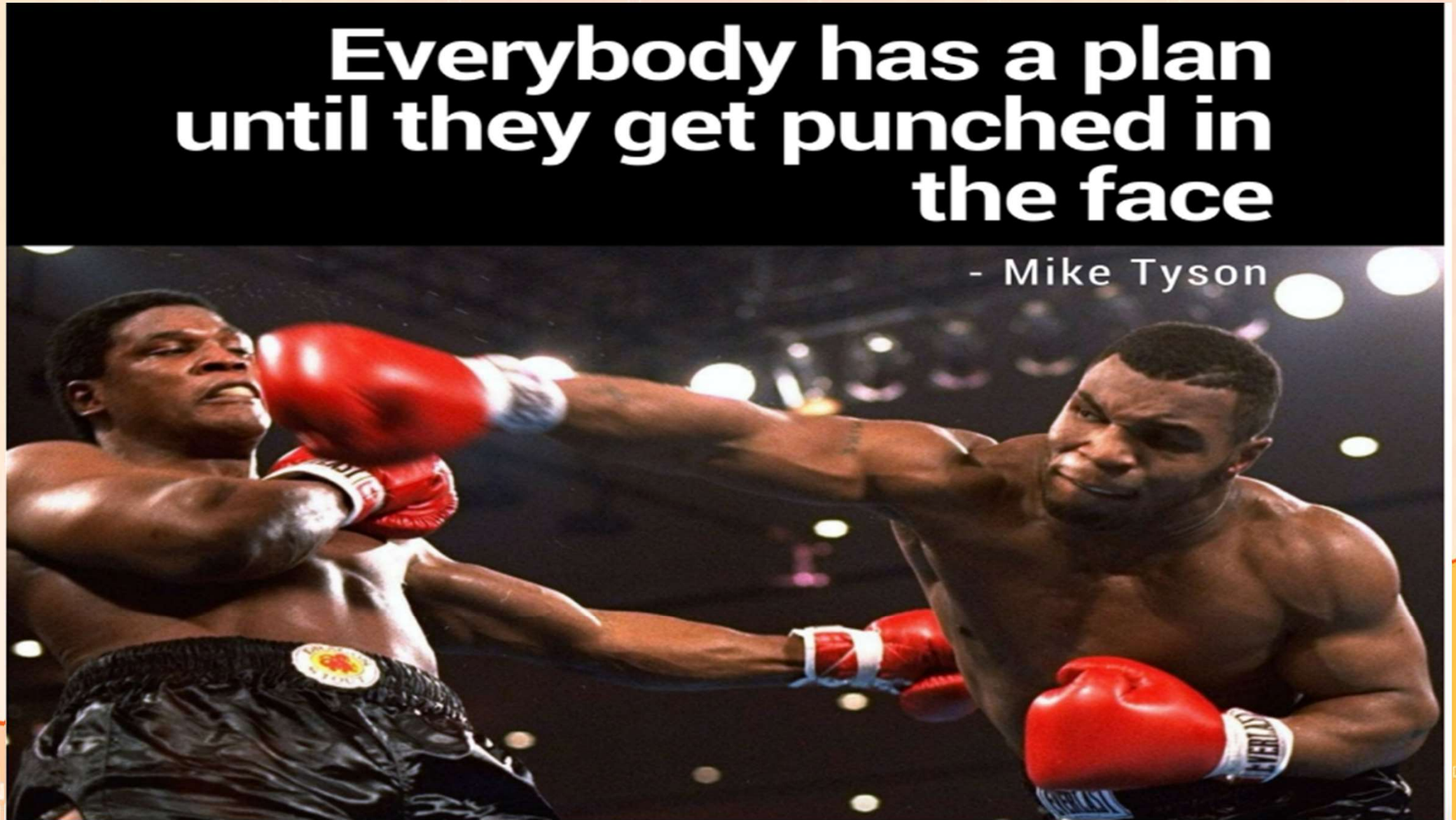
1) National Vulnerability Database https://nvd.nist.gov/

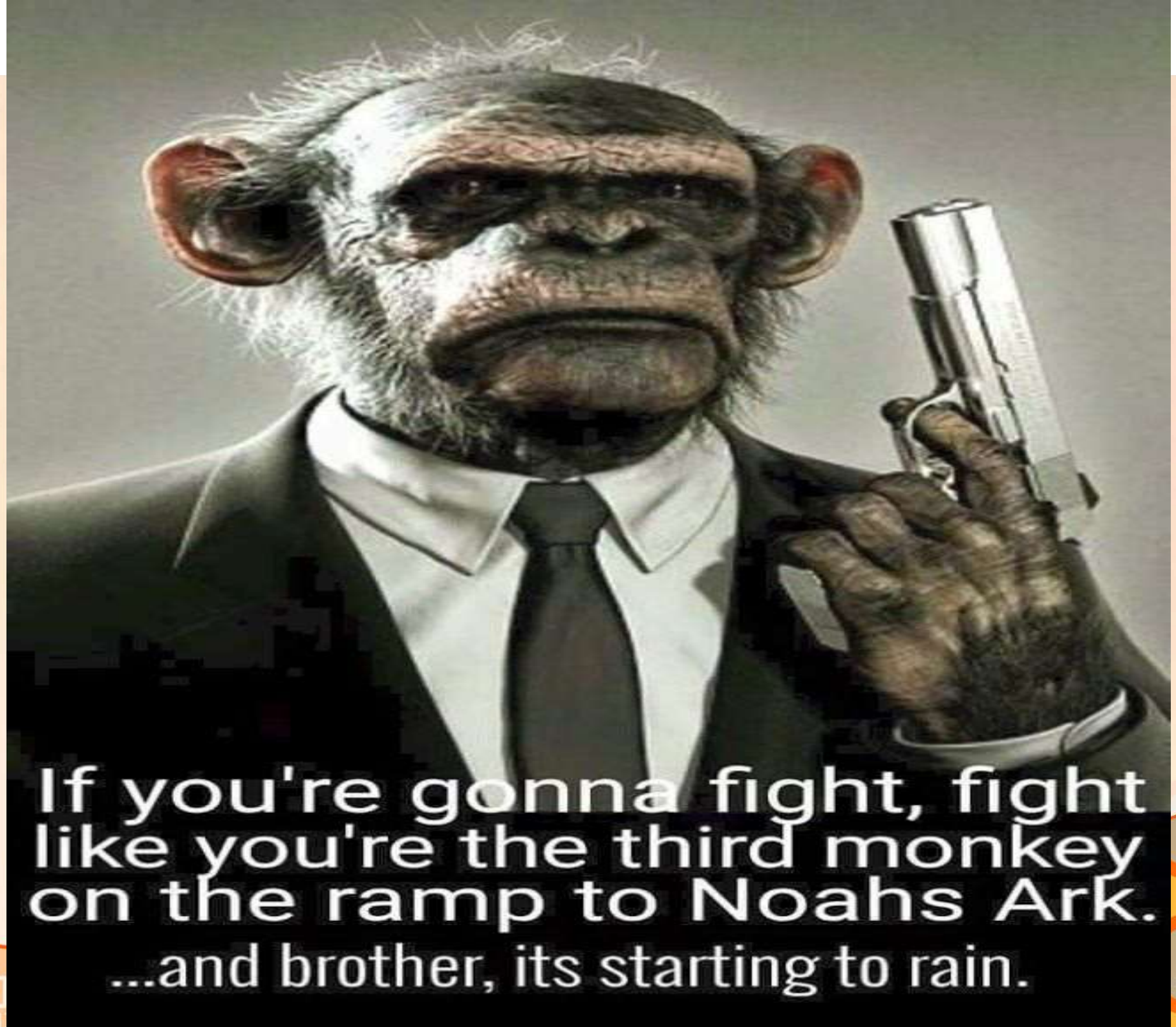
NVD i.e. National Vulnerability Database is a product of NIST (National Institute of Standards and Technology) Computer Security Division which is sponsored by DHS(Dept. of Homeland Security's). The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance.

SOURCES OF VULNERABILITY INFORMATION

- NVD
  - How many NVDs are there?
- Vendor Product Security Page
  - What if there isn't one?
- Researchers
  - How do you scale and automate this?

In 2023, YOU need to know what is out ‘there’….ahead of time and YOU need a playbook NOT just a plan to get back up!




If you're gonna fight, fight like you're the third monkey on the ramp to Noahs Ark.
...and brother, its starting to rain.