RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

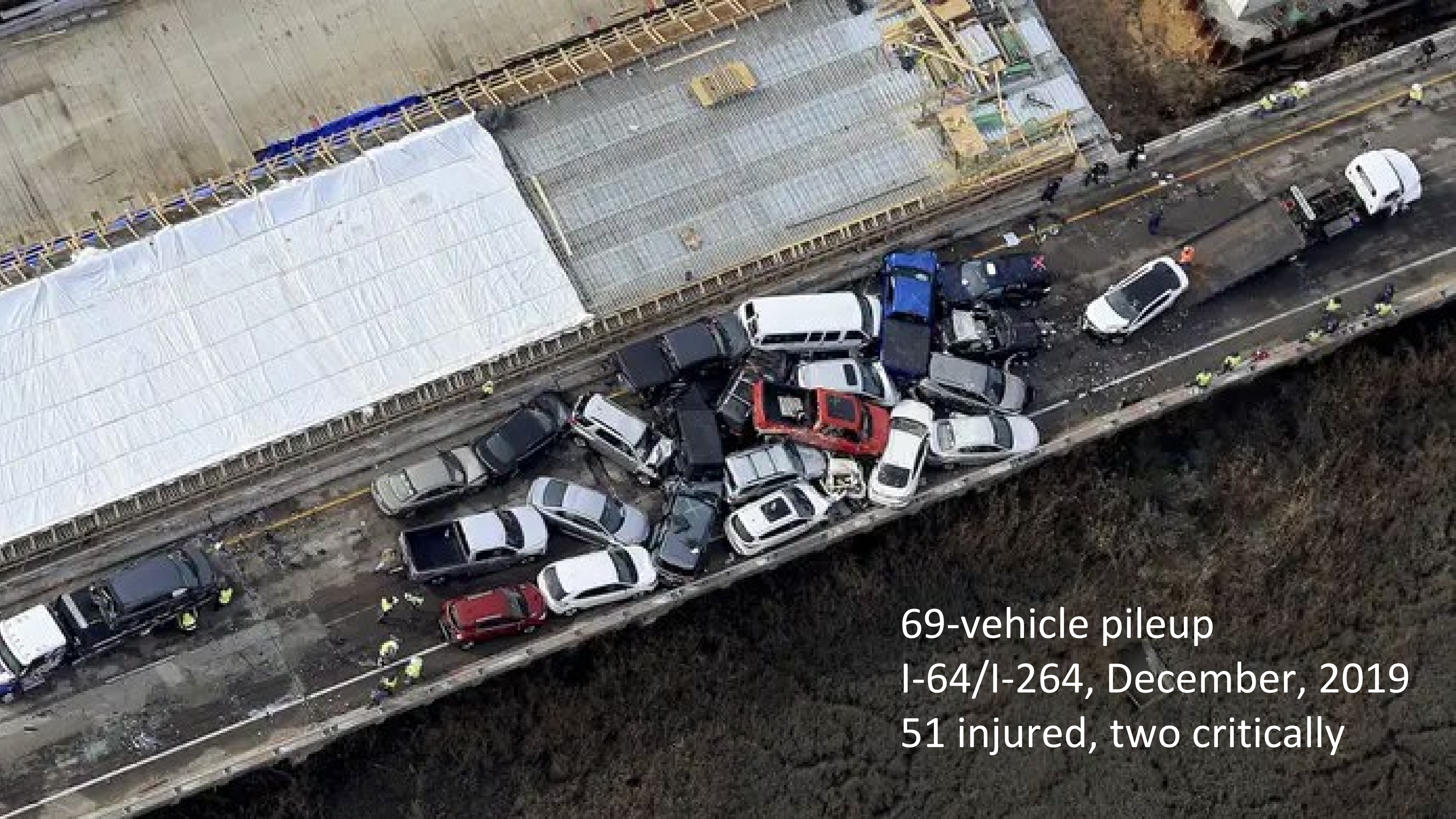
SESSION ID: **TECH-W09**

Syncopation in Enterprise IT: Uneven Migration to, and within, the Cloud

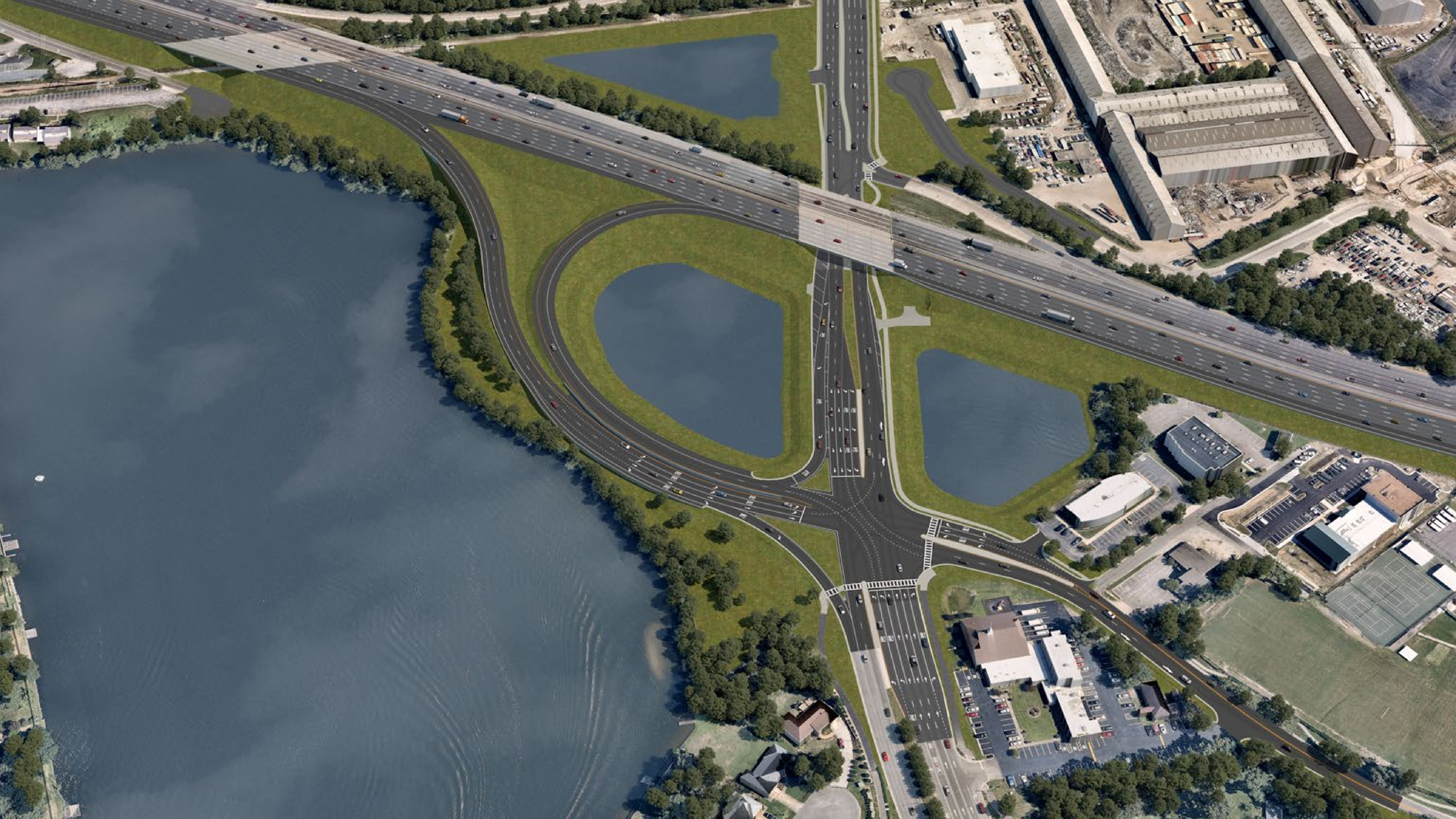
Nick Selby

Chief Security Officer, Paxos Trust Company
@fuzztech

#RSAC



69-vehicle pileup
I-64/I-264, December, 2019
51 injured, two critically



About Nick (Abridged Edition)

PAXOS Fuzz

POLICE DEPARTMENT CITY OF NEW YORK

NEW YORK POLICE DEPARTMENT INTELLIGENCE BUREAU

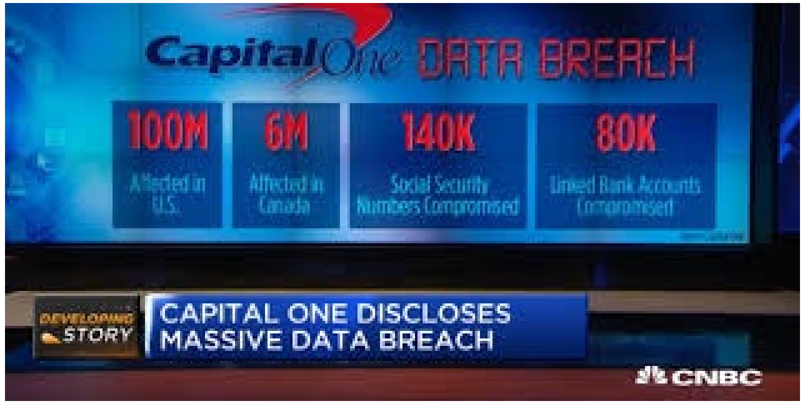
MIDLOTHIAN POLICE DEPARTMENT

CJX SecureIdeas℠

451

A Brief Word About Capital One

- Huge cloud breach; involved AWS former staff, which gives executives the heebie-jeebies.
- That this happened does not mean that AWS is unsafe, or that Capital One is incompetent. Quite the contrary.
- It means this stuff is *hard.*


Capital One DATA BREACH
100M
Affected in U.S.
6M
Affected in Canada
140K
Social Security Numbers Compromised
80K
Linked Bank Accounts Compromised
DEVELOPING STORY
CAPITAL ONE DISCLOSES MASSIVE DATA BREACH
CNBC

Super-Important Trend #1

‘No Cloud, No AI.’ – Liam Maxwell

Public cloud is changing how, and thus what, companies deliver. This is perhaps the first true paradigm shift since we all got AOL.

‘If you're going to do continuous delivery, you need an API-enabled, on-demand infrastructure at the end of the pipeline - e.g., a cloud.’ *-Chris Swan, DXC Technology*

Super-Important Trend #2

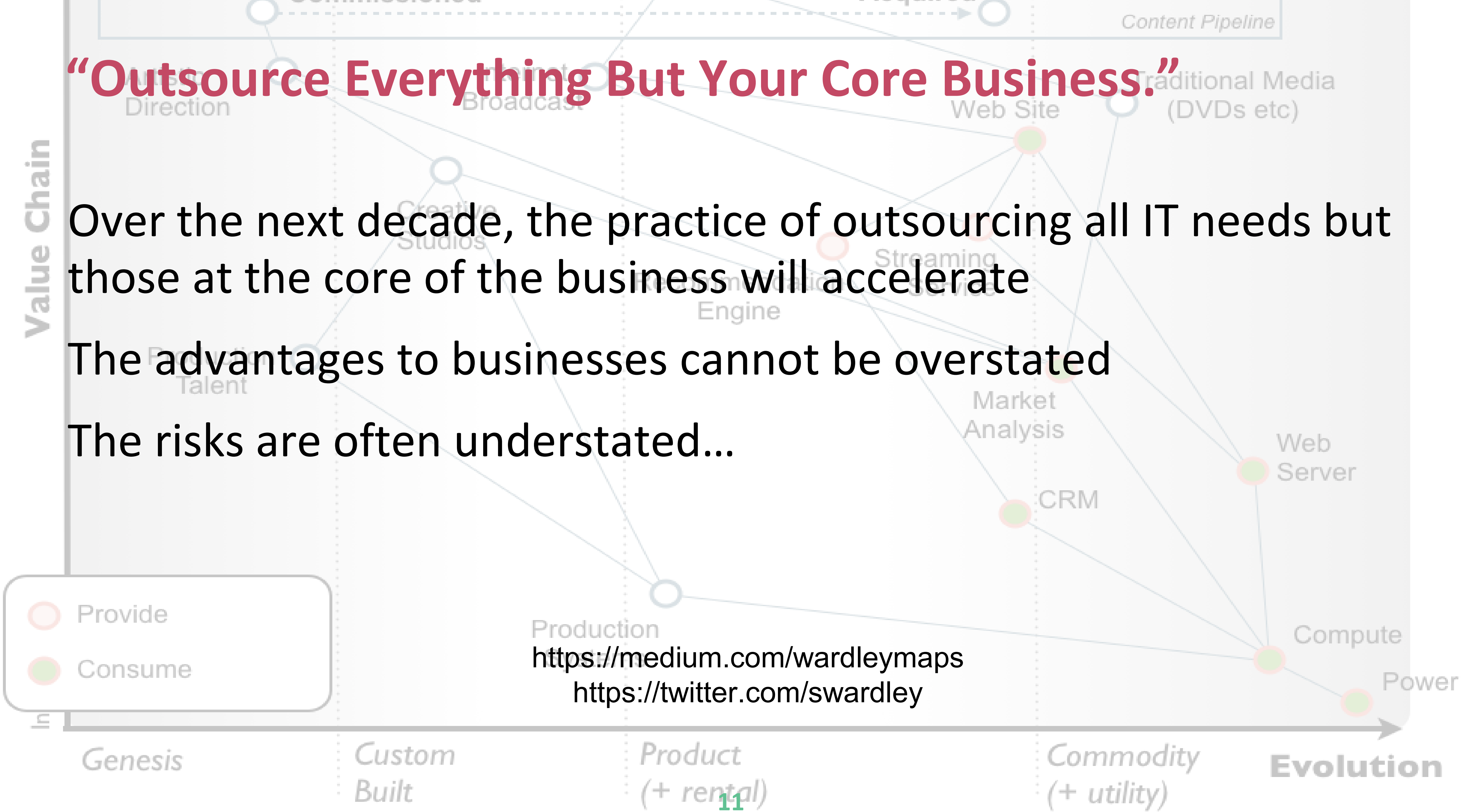
“Outsource Everything But Your Core Business.”

Over the next decade, the practice of outsourcing all IT needs but those at the core of the business will accelerate

The advantages to businesses cannot be overstated

The risks are often understated…

https://medium.com/wardleymaps
https://twitter.com/swardley



Super-Important Trend #3

Cloud Goes Native

The next decade sees companies and government moving from fork-lift-and-dump-truck migration (or, ‘Lift-and-Shift’) to native cloud deployment.

This is a decade-long project in many cases.

Chris Swan Again: Jenga v Bicycles. (https://is.gd/jengabike)

Doing This Right Brings Revolutionary Gain...

Doing this right is, like, really hard.

Doing Cloud-Native correctly means turning our backs on decades of “best practices” and abandoning millions of apps

People will become sad. Many will quit.

You’ll wish many more quit.

It will never be easier or cheaper than it is today.

To quote Clint Bruce, SEAL Team 5 Commander...

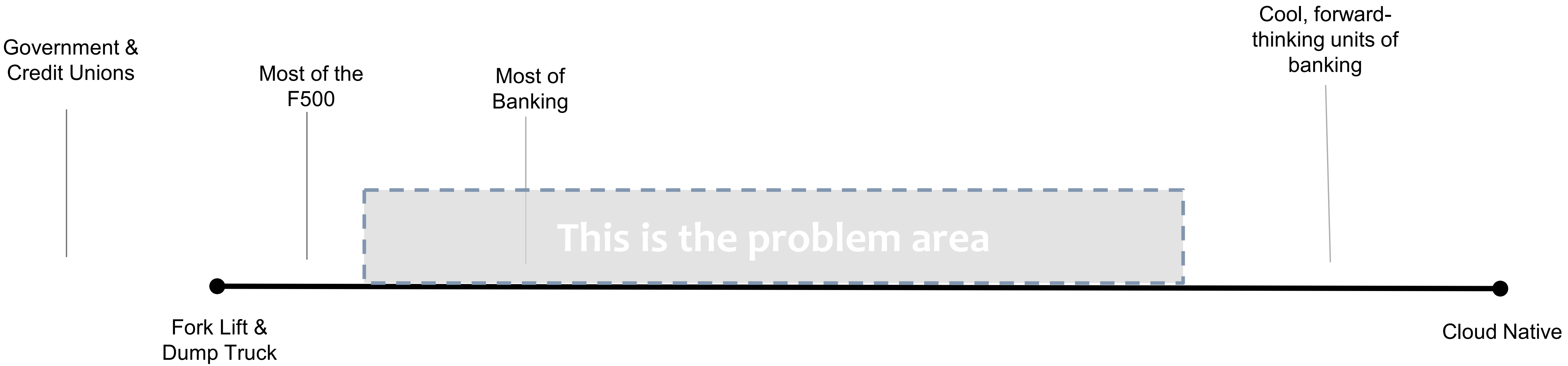
Apply: Cloud Strategy is IT Strategy

Right After RSA: Ask yourself about the maturity of your strategy to migrate to, and within the cloud. Is it a data-center in the sky?

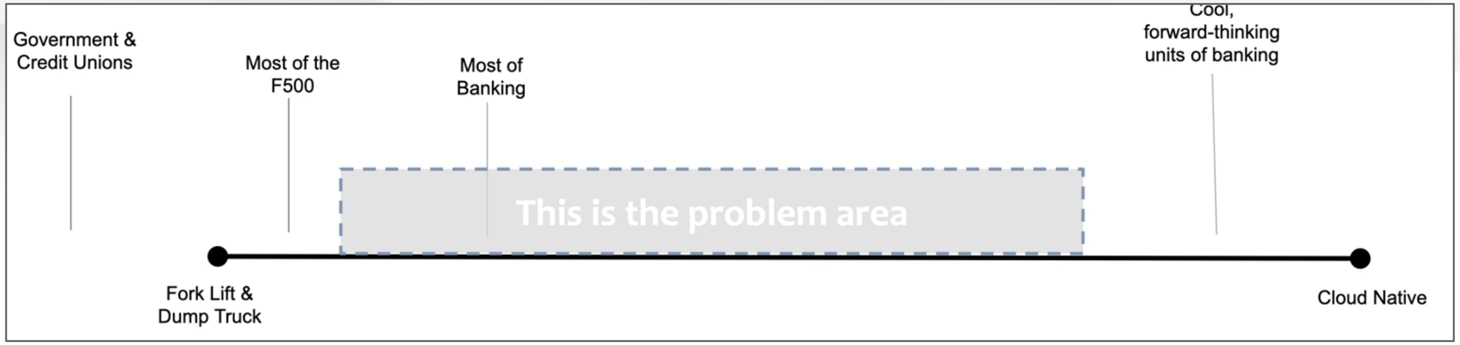
- Are you still doing CapEx versus OpEx presentations?
- How have you articulated strategically the fundamental changes that your IT fabric will traverse when you commit fully to cloud-native?
  - This would include an understanding by HR of the **cultural shifts** inherent in this move

Finding Your Place

The Continuum



The Continuum

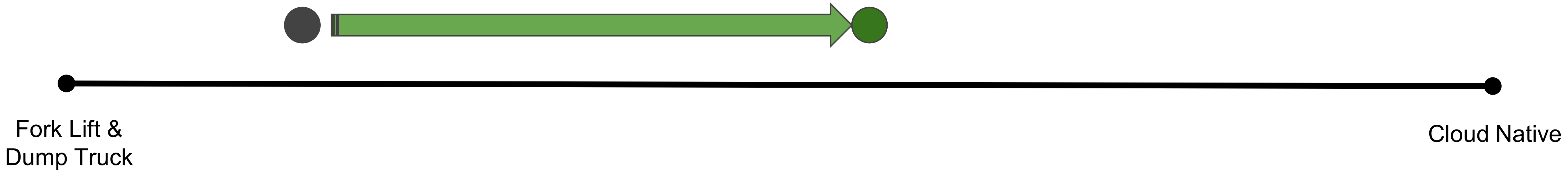


Wherever you are on the continuum, that’s cool.

The problems begin when you start to move rightward.

Moving Rightward On The Continuum

Segregation
Developer access
Prod and non-prod environments
Configuration/Automation
Access control and Authorization
API access, internal and external
Backup and storage
Logging
Integration with existing technology
Integration with future technology



This Is A Cultural Challenge As Much As A Technical One.

We want cool features.

Building features is super-fun.

Building foundational stuff is super-boring.

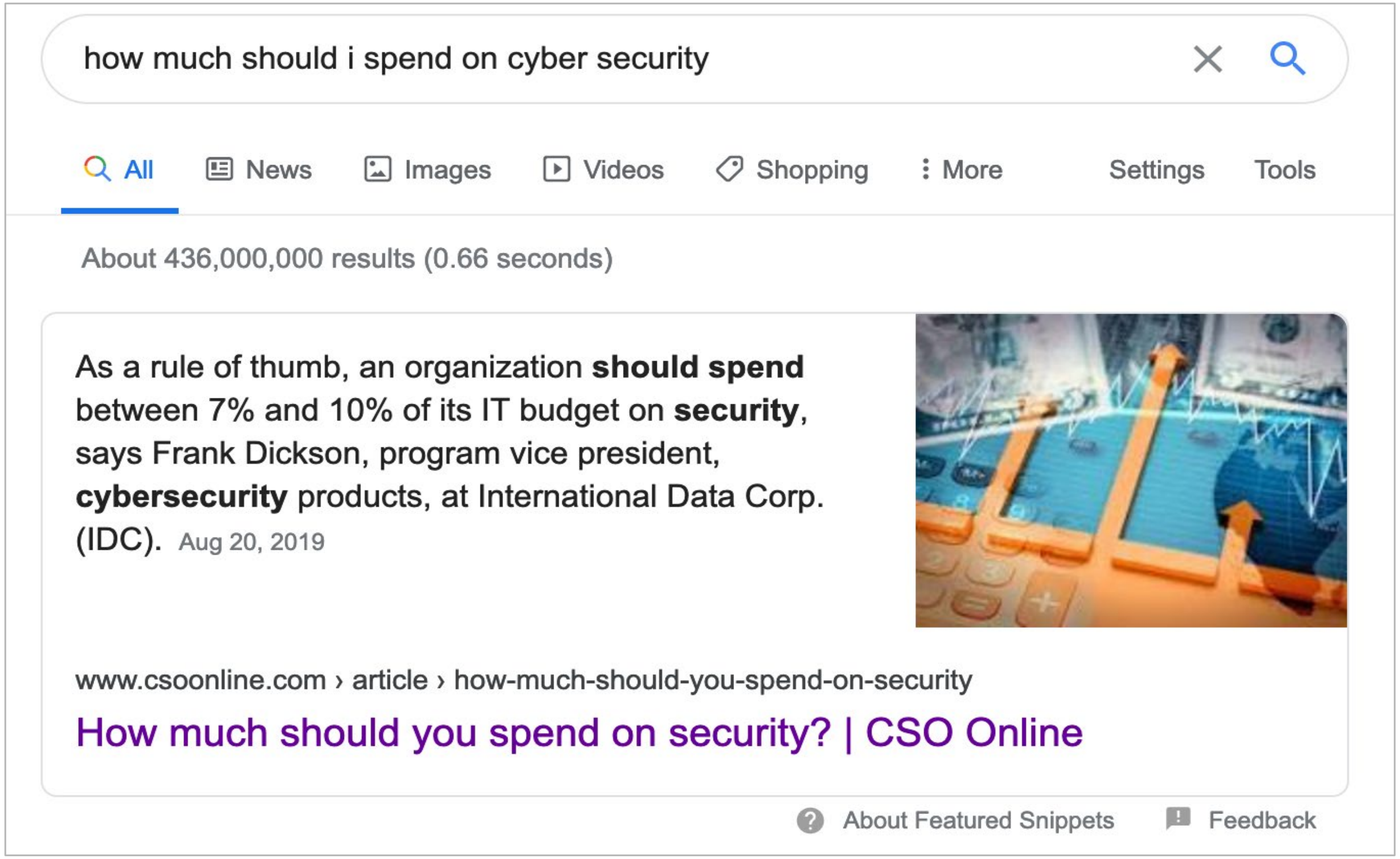
Engineers and product managers want super-fun stuff.

Only security people want super-boring foundational stuff.

This Is A Cultural Challenge As Much As A Technical One.

Executives don’t understand the choices they’re being given.

With no good choices, executives make arbitrary decisions.



how much should i spend on cyber security

About 436,000,000 results (0.66 seconds)

As a rule of thumb, an organization **should spend** between 7% and 10% of its IT budget on **security**, says Frank Dickson, program vice president, **cybersecurity** products, at International Data Corp. (IDC). Aug 20, 2019

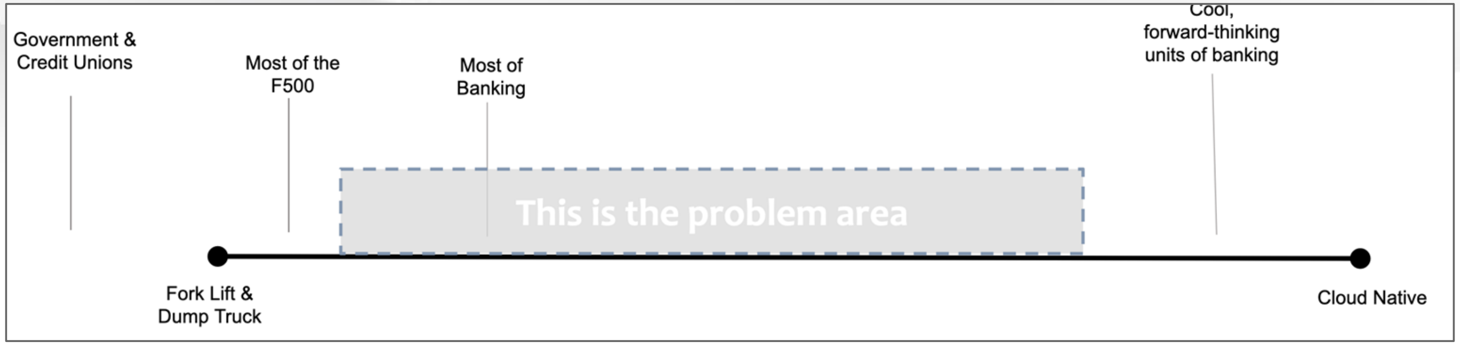
www.csoonline.com › article › how-much-should-you-spend-on-security

How much should you spend on security? | CSO Online

With no good choices, executives make arbitrary decisions.

Bad choices in the cloud give you cloud-enabled stupid, delivered at cloud speed.

The Continuum



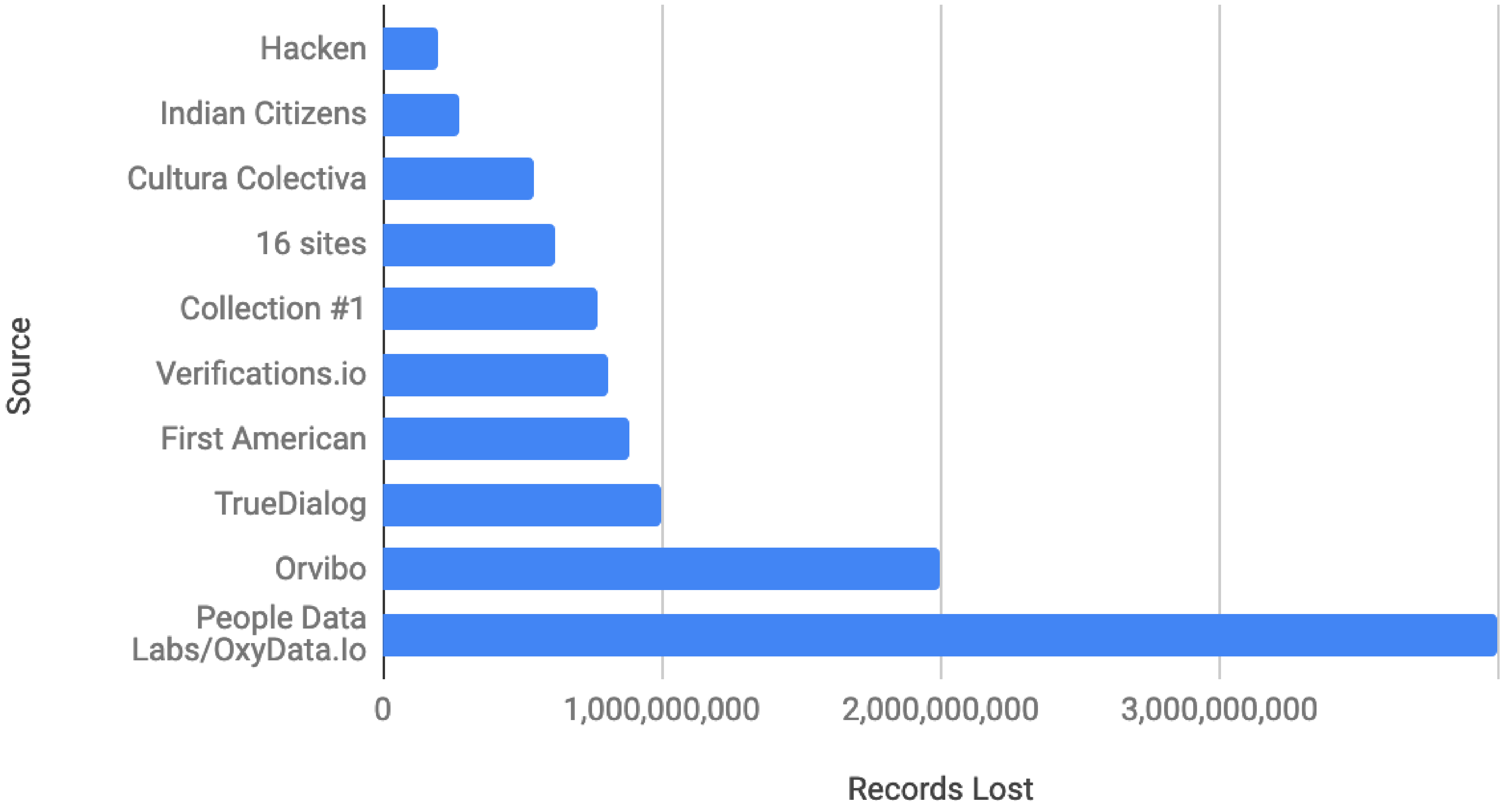
Companies can’t acquire their way out of this.

- Most of the companies they would buy are on the left.
- Many outsourced solutions are on the left.
- Except for the startups.

This means that, for the next ten years, third party risk is the biggest single problem faced by enterprise IT executives (more on that later)

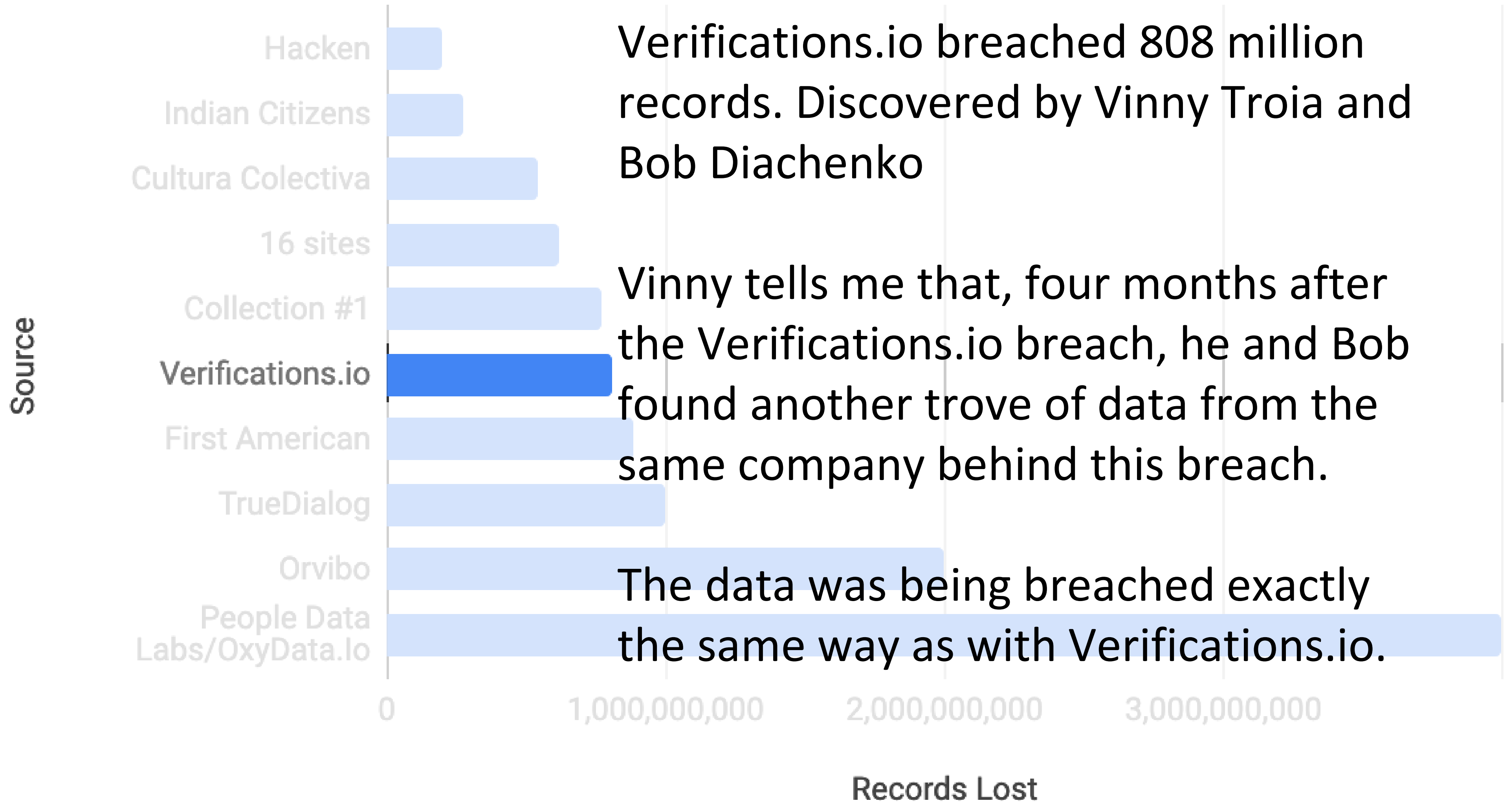
Rubber Meeting The Road

Top Ten Data Breaches By Records Lost, 2019



Data: HaveIBeenPwned.com, thanks, Troy!

Top Ten Data Breaches By Records Lost, 2019



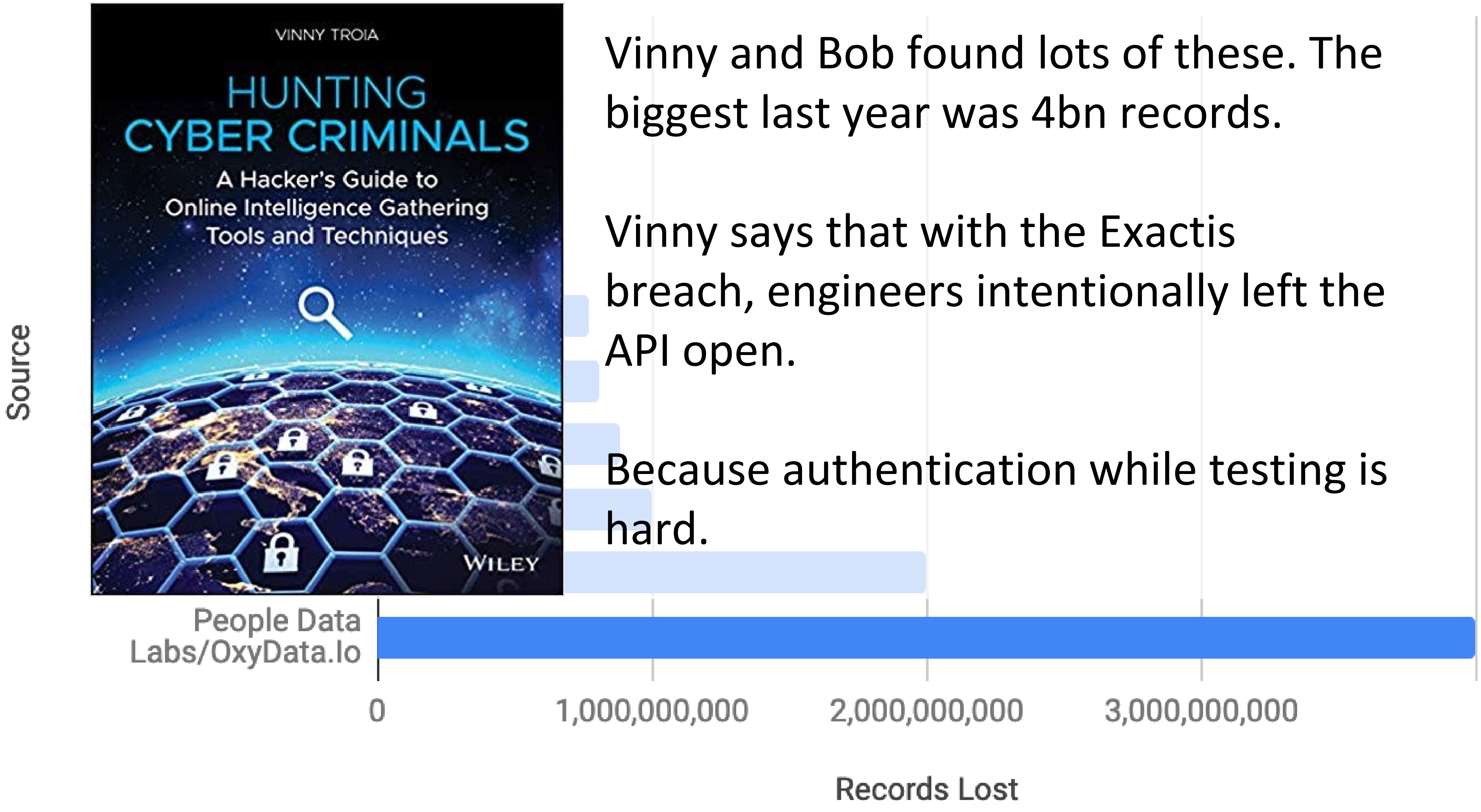
Verifications.io breached 808 million records. Discovered by Vinny Troia and Bob Diachenko

Vinny tells me that, four months after the Verifications.io breach, he and Bob found another trove of data from the same company behind this breach.

The data was being breached exactly the same way as with Verifications.io.

Data: HaveIBeenPwned.com, thanks, Troy!

Top Ten Data Breaches By Records Lost, 2019



Vinny and Bob found lots of these. The biggest last year was 4bn records.

Vinny says that with the Exactis breach, engineers intentionally left the API open.

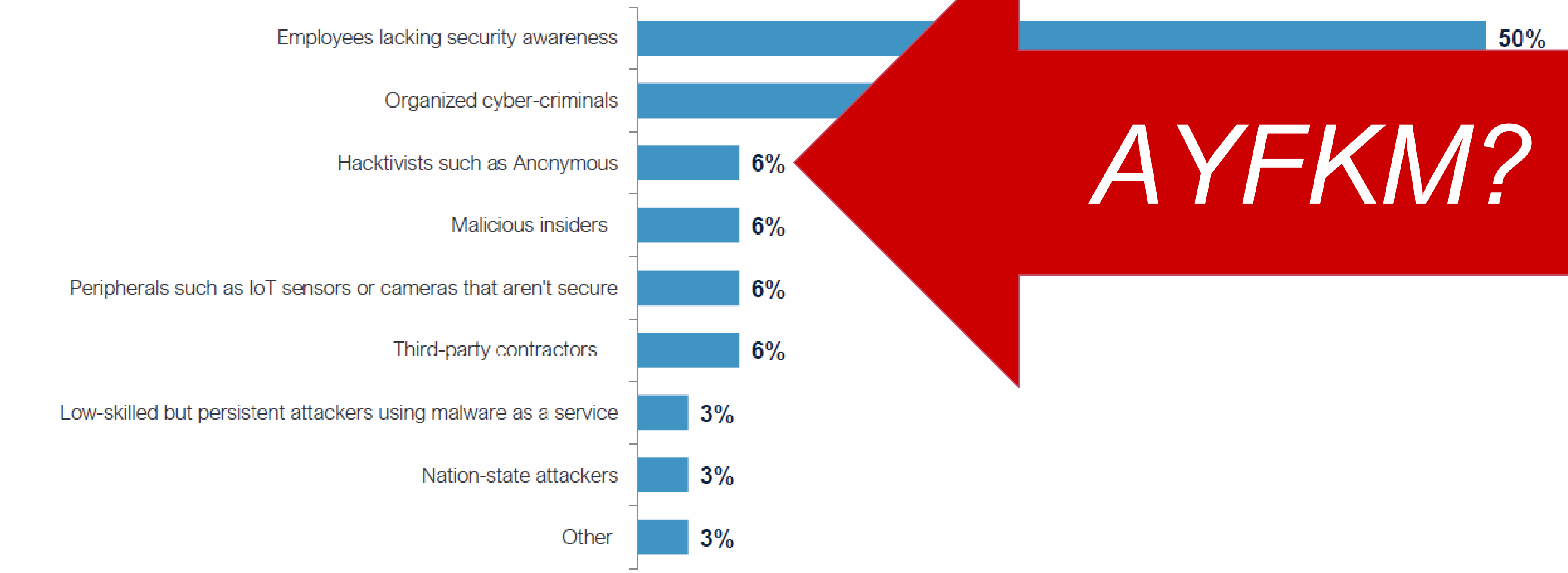
Because authentication while testing is hard.

Data: HaveIBeenPwned.com, thanks, Troy!

And what do security professionals think?

Single Greatest Security Threat

When forced to identify the single greatest threat to security, respondents were most likely to identify a lack of security awareness among employees (50%), followed at a distance by organized cyber-criminals (18%).

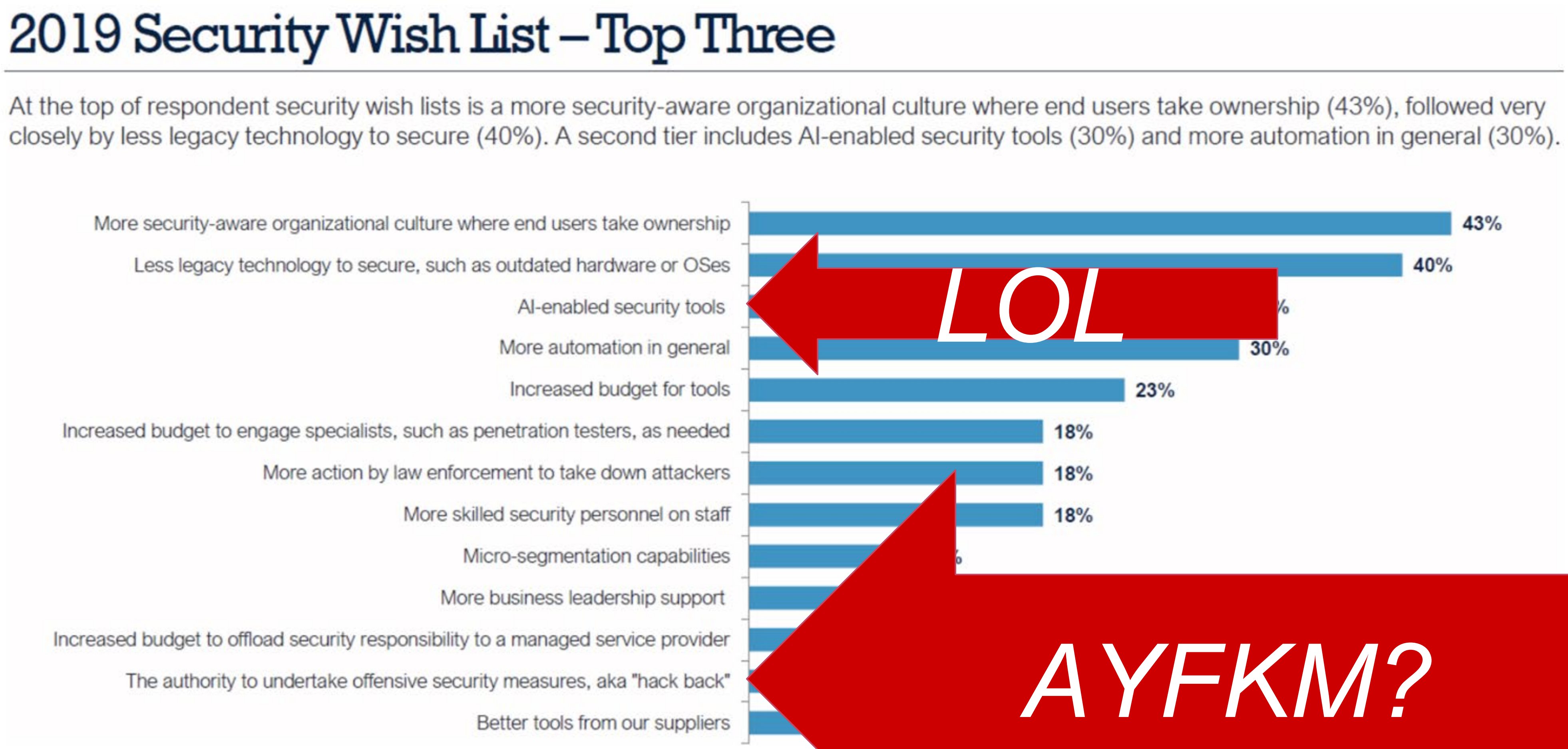


AYFKM?

!?

Data Center Knowledge/ Informa Tech family of sites, **2019 survey** of security professionals.

And what do security professionals think?



2019 Security Wish List – Top Three

At the top of respondent security wish lists is a more security-aware organizational culture where end users take ownership (43%), followed very closely by less legacy technology to secure (40%). A second tier includes AI-enabled security tools (30%) and more automation in general (30%).

More security-aware organizational culture where end users take ownership	43%
Less legacy technology to secure, such as outdated hardware or OSes	40%
AI-enabled security tools	%
More automation in general	30%
Increased budget for tools	23%
Increased budget to engage specialists, such as penetration testers, as needed	18%
More action by law enforcement to take down attackers	18%
More skilled security personnel on staff	18%
Micro-segmentation capabilities	%
More business leadership support	
Increased budget to offload security responsibility to a managed service provider	
The authority to undertake offensive security measures, aka "hack back"	
Better tools from our suppliers	

LOL

AYFKM?

!?

ter nowledge/
fec family o sites,
vey of securi
nal

Apply: What's Important To You?

Right After RSA: Look at your last five significant security events or incidents, and their root causes. Do your personal views on what is important to your security map well to those root causes?

Three Months Out: Do the same thing.

Six Months Out: Make a strategy to articulate these important things, in plain business English, to leadership.

If You Think That Isn’t Funny,
Here’s Something That Isn’t Even Funnier…
Third Party Risk

In This Context, Let Us Consider Third Party Risk.

A survey of 608 decision makers from Professional Services, Finance, Manufacturing, Healthcare, Retail and the Public Sector:

- 89 vendors are accessing their company's network every single week.
- 75% saw access by third parties grow in the past 24 months.

This was in 2016.

And remember….

We are, all of us, outsourcing that which is not our core competency.

Payroll
Health benefits
Human Resources
Trouble Ticketing
Accounting
Bill paying
Customer Relationship
Management
Account reconciliation

IT management
IT Security management
IT Security monitoring
Log management
Firewall management
Employee tech onboarding
Secure messaging
Business process management

Drafting
Translation services
Marketing
Web design
Recruitment
Sales lead management
IT Response (alert management)
Banking

If Everyone Is In This Cloudy Boat

Since everyone is making these same kinds of decisions, everyone has holes in their intra-cloud migration strategy.

We're trusting with our data vendors who are on this same journey; vendors who have made tradeoffs (as we all do) as to what to implement first: security or product features (as if the former isn't the latter)

This leads to some new kinds of procurement challenges...

A Case Study in Outsourcing: Payroll

Which cloud-based payroll processor supports TOTP application-based MFA for login?

ADP®

PAYCHEX®

SUREPAYROLL
A PAYCHEX® COMPANY

GUSTO

JUSTWORKS.

So, I Sign Up For JustWorks.

On the second day, after all sorts of configuration, I need to change something complex, so I call their toll-free customer support number.

I tell them what I need to accomplish.

They say...

The Most Dreaded Words I Can Hear:

"For security purposes, please tell me your full name, and the last four digits of your Social Security Number…"

Everyone Moves Rightward At A Different Speed

The other payroll companies don’t consider (non-SMS-based) MFA to be an important feature *for their customers.*

If customers don’t specifically ask, it’s “not important.”

We know of a SIM-swap based attack last month that leveraged phone-based password reset to target institutional trading accounts.

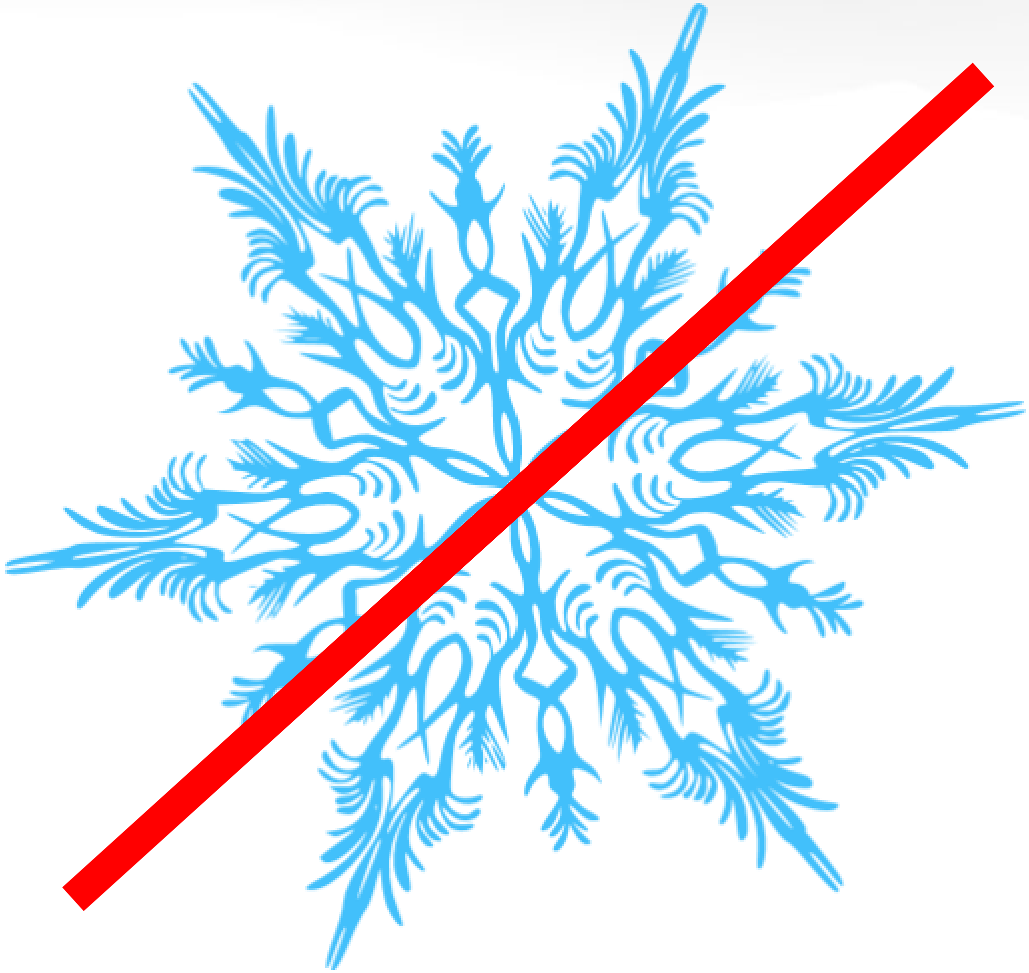
So the question becomes, “Does your vendor vetting program ask about password reset?”

Some Vendor Onboarding Truths

Many companies think about the data they entrust to a TP provider in levels, like low, medium, or high, or 1, 2, and 3.

As Aaron Turner used to say, “Data is protected or it is not.” There are no “levels.”

As breaches have taught us, we can’t plan what data types are important to thieves.



Rethink Your Vendor Onboarding Vetting Process

Spreadsheets are fine, but are the questions you're asking made for another era?

Do they assume the vendor is in the cloud, or that they're not?

- Example: Do you ask whether the vendor has separate prod and non-prod environments? If developers need MFA and VPN to get into their cloud? How they detect unencrypted S3 buckets? How they automate deployment?
- These are more impactful answers than that to, "Do you have a firewall?"

Apply: Third Party Risk Assessment

After The Conference: Review your presumptions about TPR, and the questionnaires and spreadsheets you use to qualify vendors.

Within 3 Months: Prepare program revamps for new vendor onboarding based on the assumptions that outsourced solutions are cloud based, and they've got your data.

Within 1 Year: Begin a program to review ex-post-facto your entire vendor stable under these new criteria.

Summary

“The cloud” is safe. We are human. “Safe” doesn’t mean what we think.

Configuration, more than ever, is everything.

If you are not standardizing deployment, creating infrastructure-as-code; and testing all your configuration assumptions, you are committing Cloud-Enabled Stupid, deployed at Cloud Speed.

This is where the distinction between ZeroTrust and “Basic cloud computing configuration” becomes key.

It will never be cheaper or easier than it is today to get this right.

RSA®Conference2020

Thank You!

Nick Selby

nselby@paxos.com

@fuzztech