RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

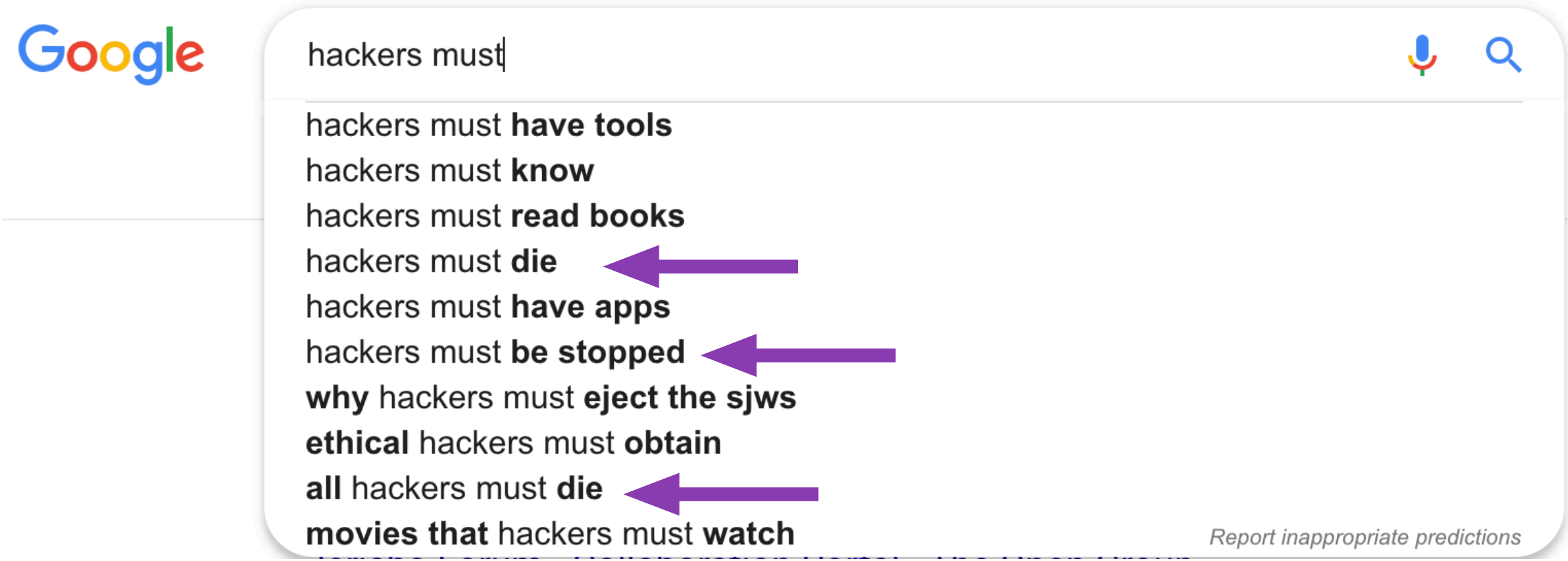
SESSION ID: GPS-R03

Countering Attacks From The Digital Horde

Dave Lewis

Global Advisory CISO
Cisco Systems
@gattaca

WHOAMI


Google
hackers must
hackers must have tools
hackers must know
hackers must read books
hackers must die
hackers must have apps
hackers must be stopped
why hackers must eject the sjws
ethical hackers must obtain
all hackers must die
movies that hackers must watch
Report inappropriate predictions


CISCO

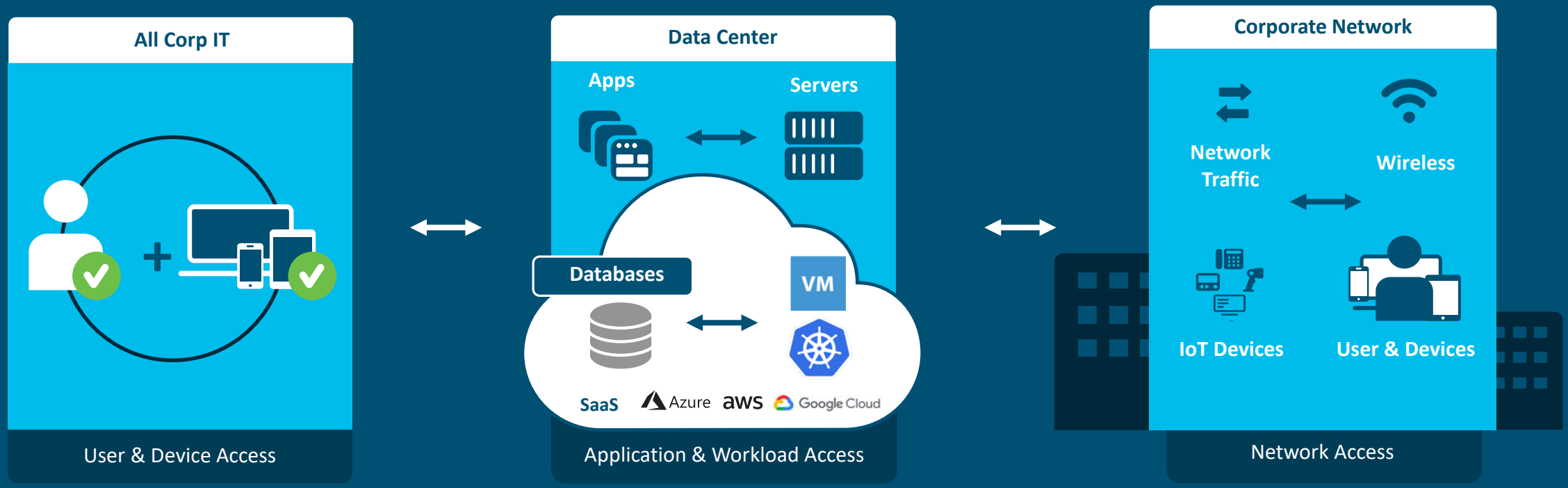
Securing the Enterprise

Access happens everywhere – how do you get visibility & ensure secure, trusted access?

Workforce

Workload

Workplace



Know Thyself…

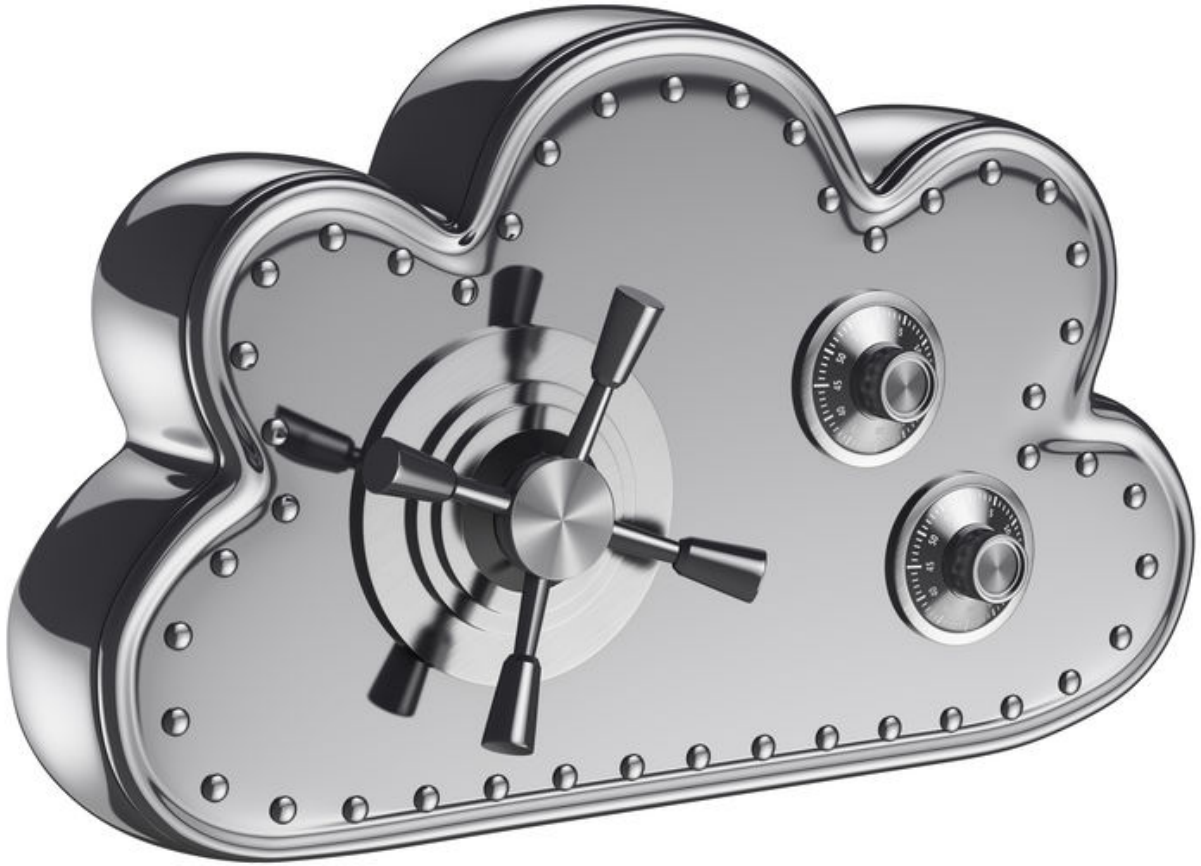
Educational Programs

Audit All The Things!

- Testing your breach incident response plan
- Risks and benefits of information sharing
- Often Compliance is the adult in the room

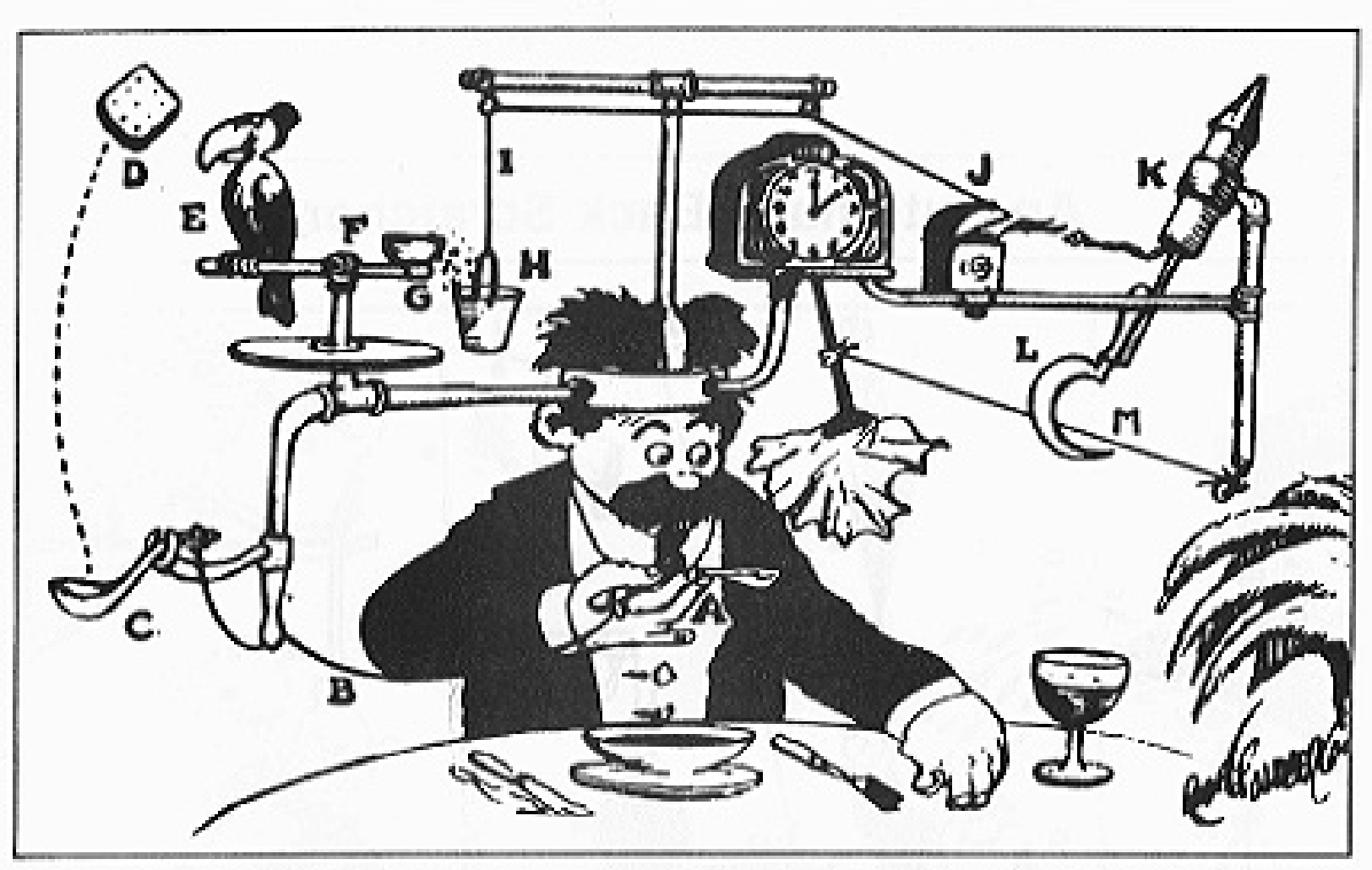
The Risk Register

Encrypt Your Data

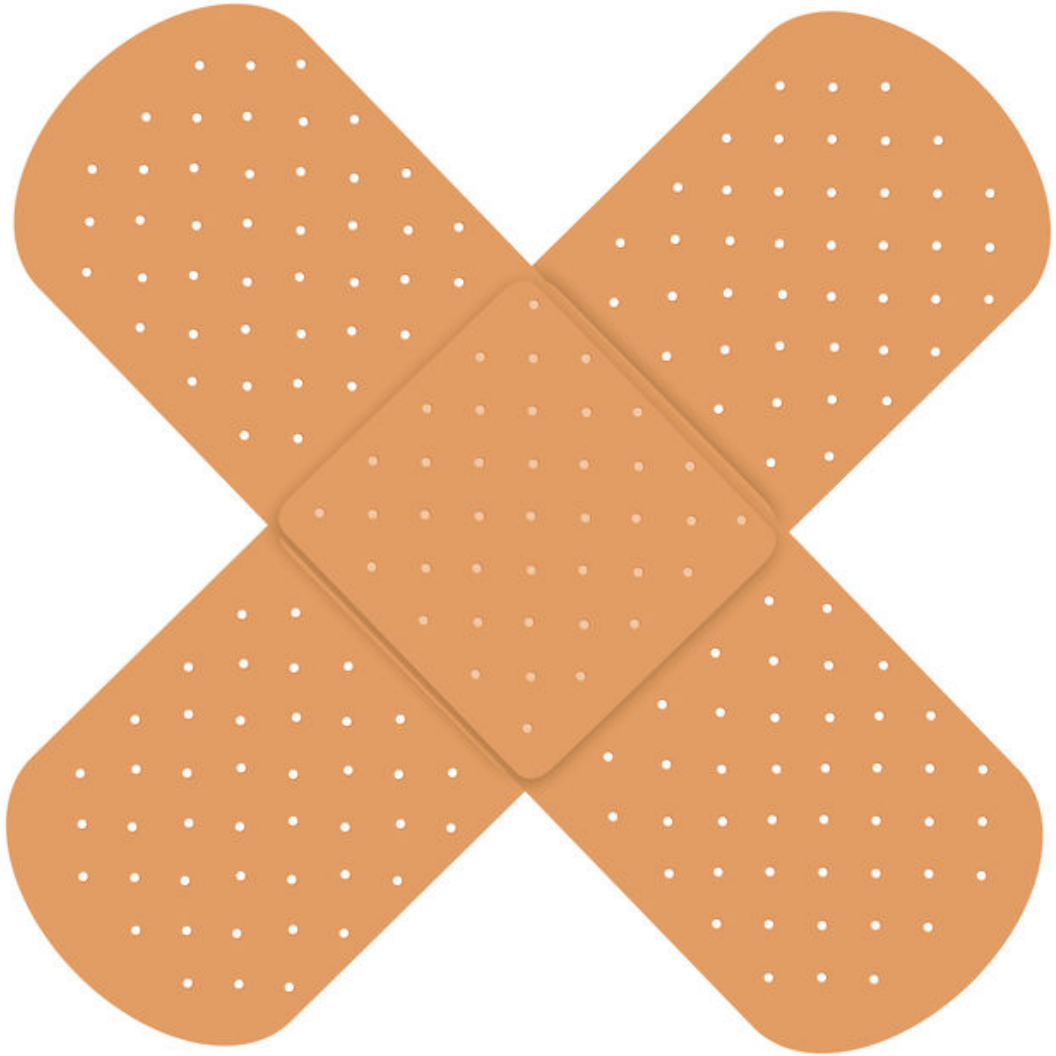


Backup, Backup, Backup…and Test Them

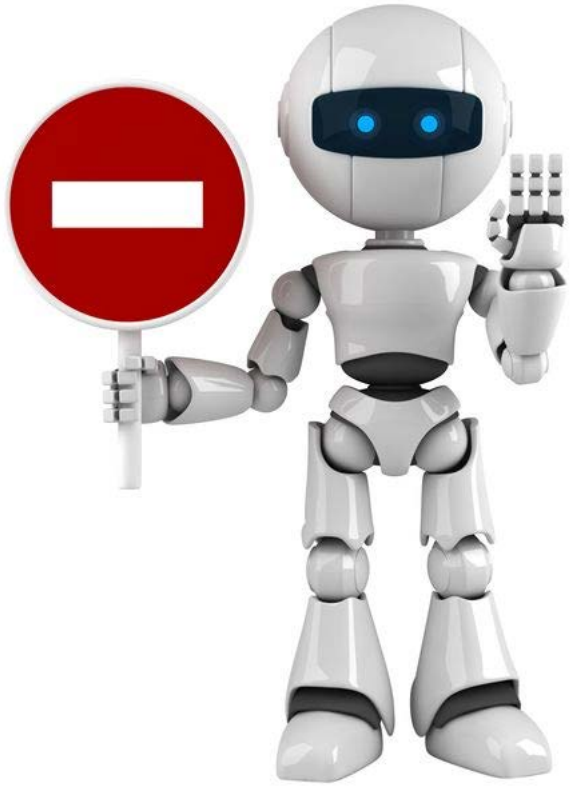
Defined Repeatable Process

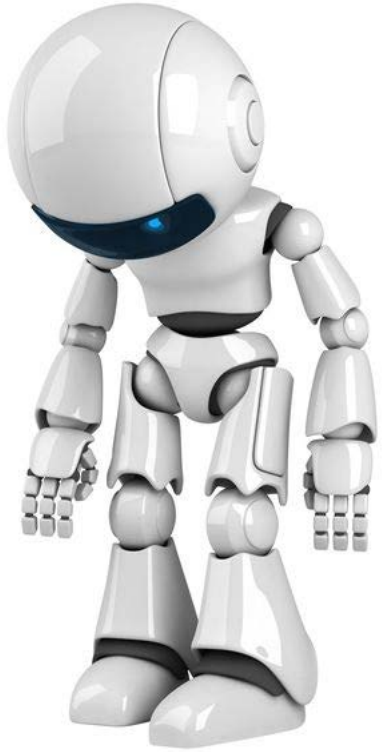


Patch Management



Time To Say Goodbye To Passwords



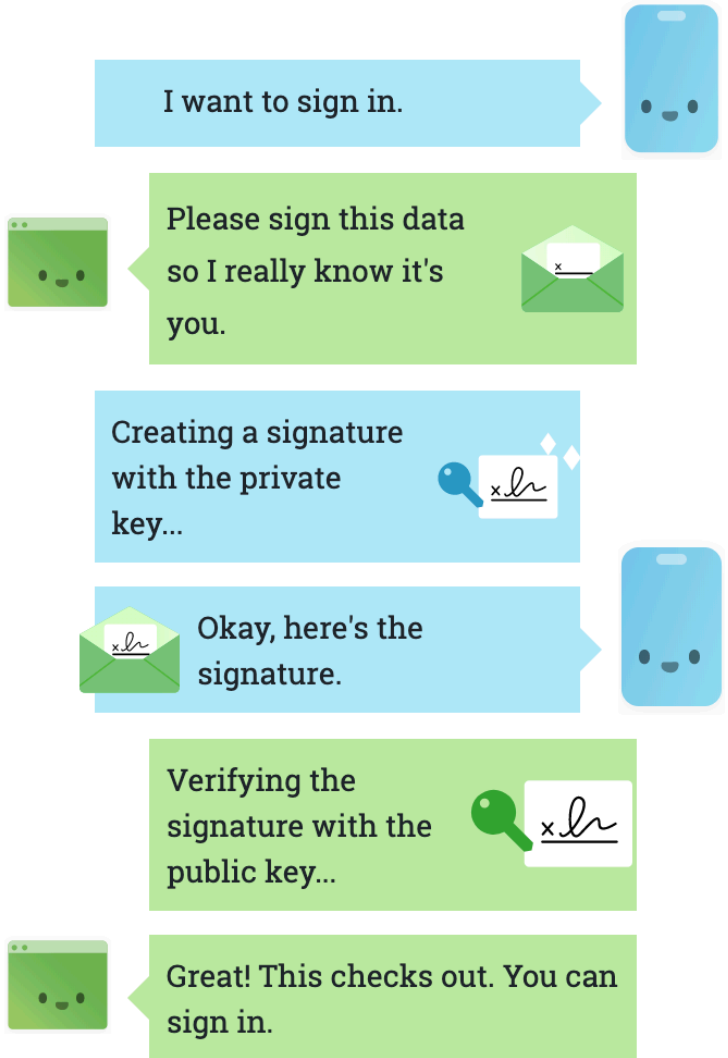


Multifactor Authentication

WebAuthn

Authenticating with a WebAuthn Credential

After registration has finished, the user can now be authenticated. During authentication an *assertion* is created, which is proof that the user has possession of the private key. This assertion contains a *signature* created using the private key. The server uses the public key retrieved during registration to verify this signature.



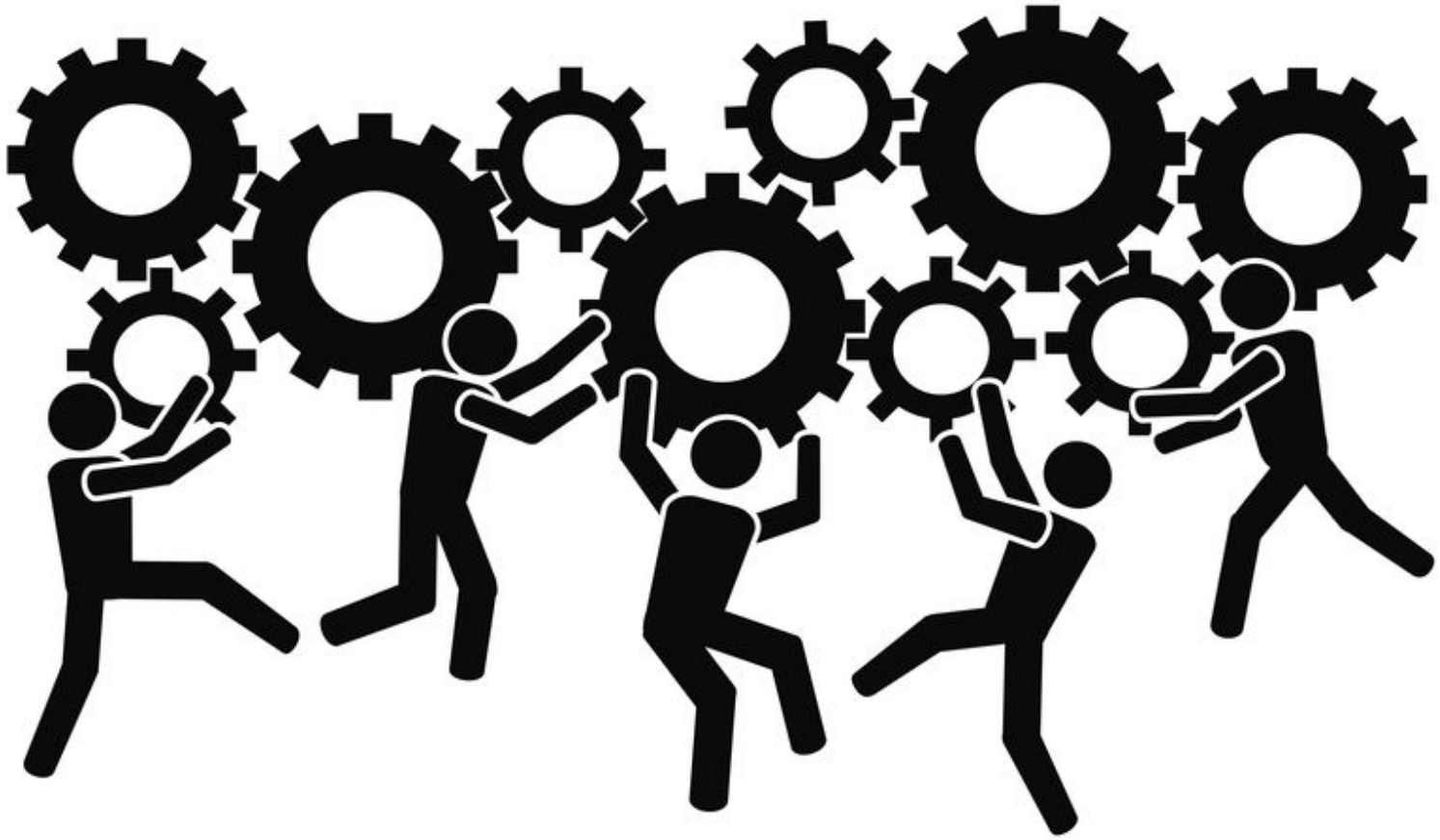
Verification will look different depending on the language and cryptography library used on the server. However, the general procedure remains the same.

```
const storedCredential = await getCredentialFromDatabase(
    userHandle, credentialId);

const signedData = (
    authenticatorDataBytes +
    hashedClientDataJSON);

const signatureIsValid = storedCredential.publicKey.verify(
    signature, signedData);

if (signatureIsValid) {
    return "Hooray! User is authenticated! 🎉";
} else {
    return "Verification failed. 😭"
}
```


WebAuthn.io
A demo of the WebAuthn specification

- Do you really need that data?
- Is that data encrypted?
- Is the data safely controlled?
- Roll out a retention policy.

Cross Organizational Teams



Protect The Workforce

Protect The Workload

Protect The Workplace

Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.

Targeting Identity

81% of breaches involved compromised credentials

Targeting Apps

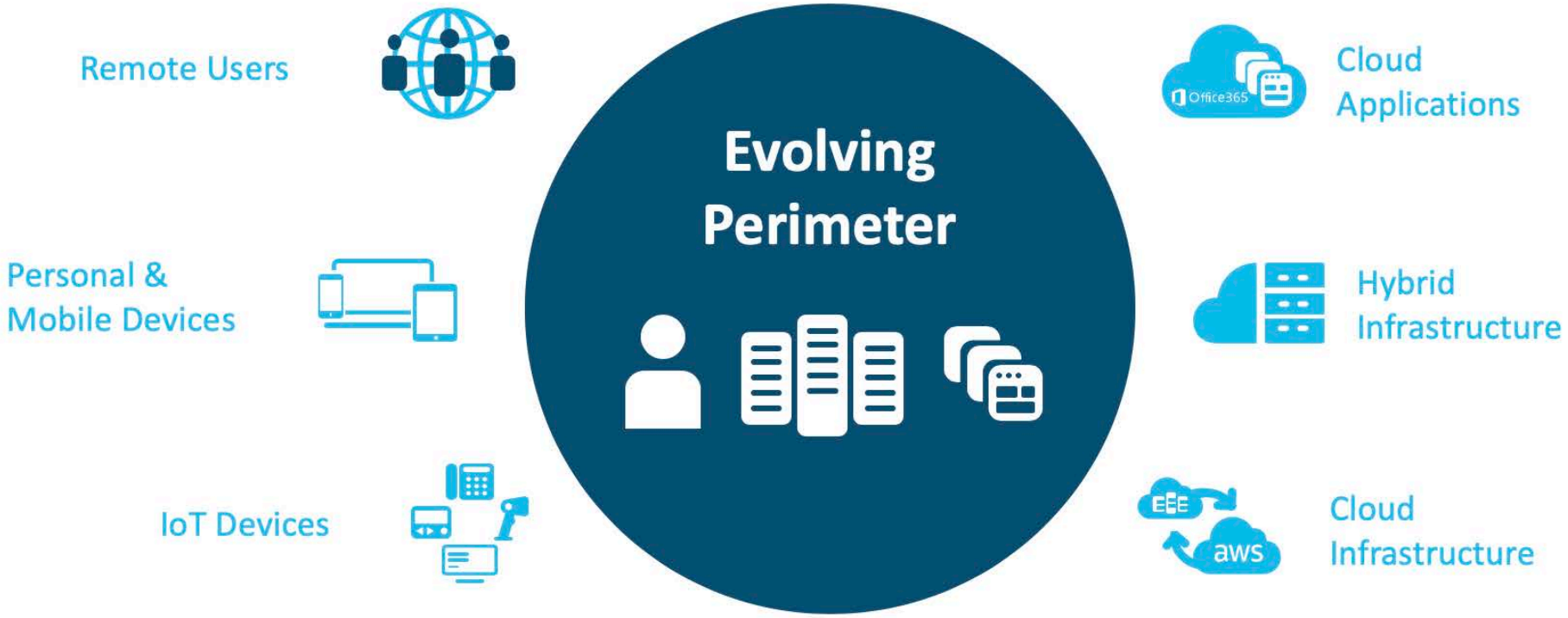
54% of web app vulnerabilities have a public exploit available

Targeting Network

92% of external pentests led to a breach of network perimeters

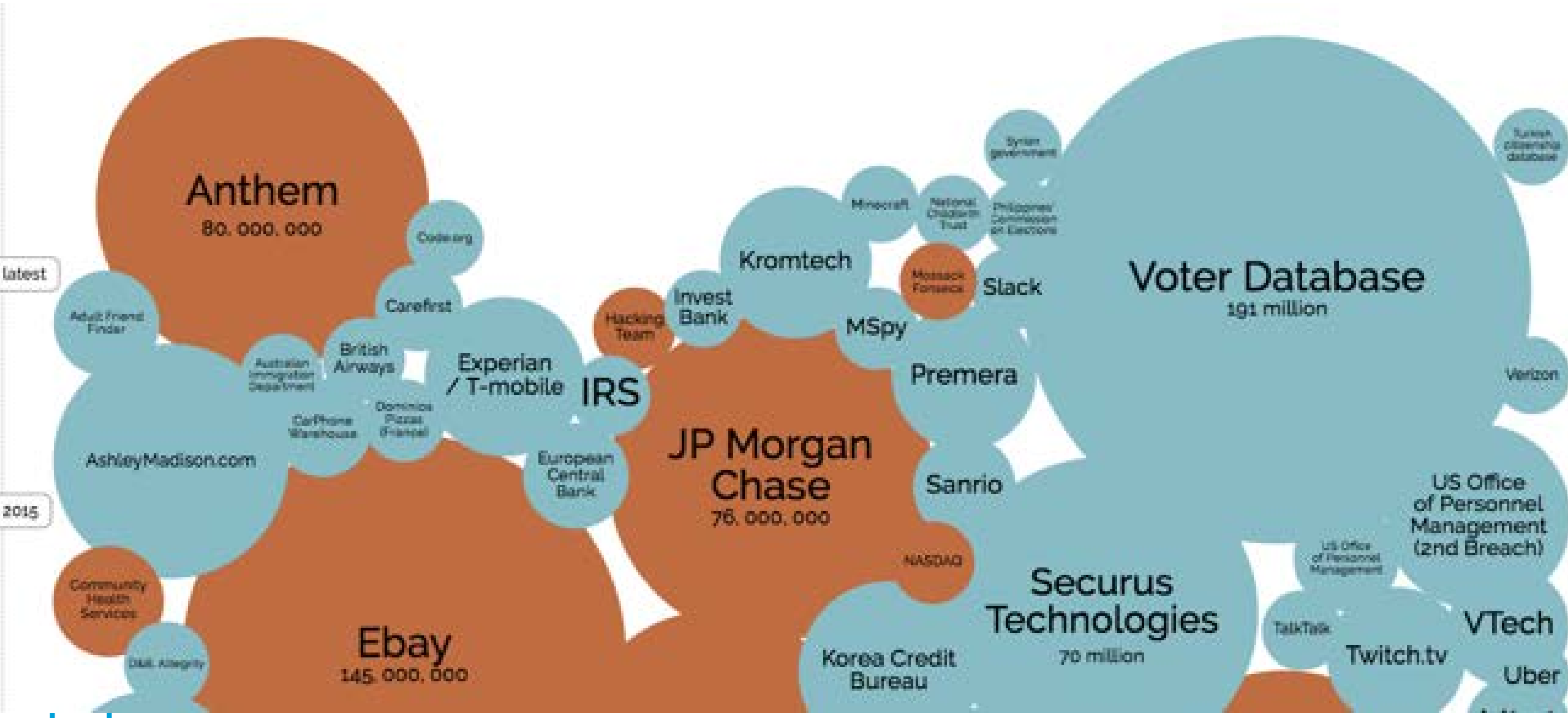
CISCO

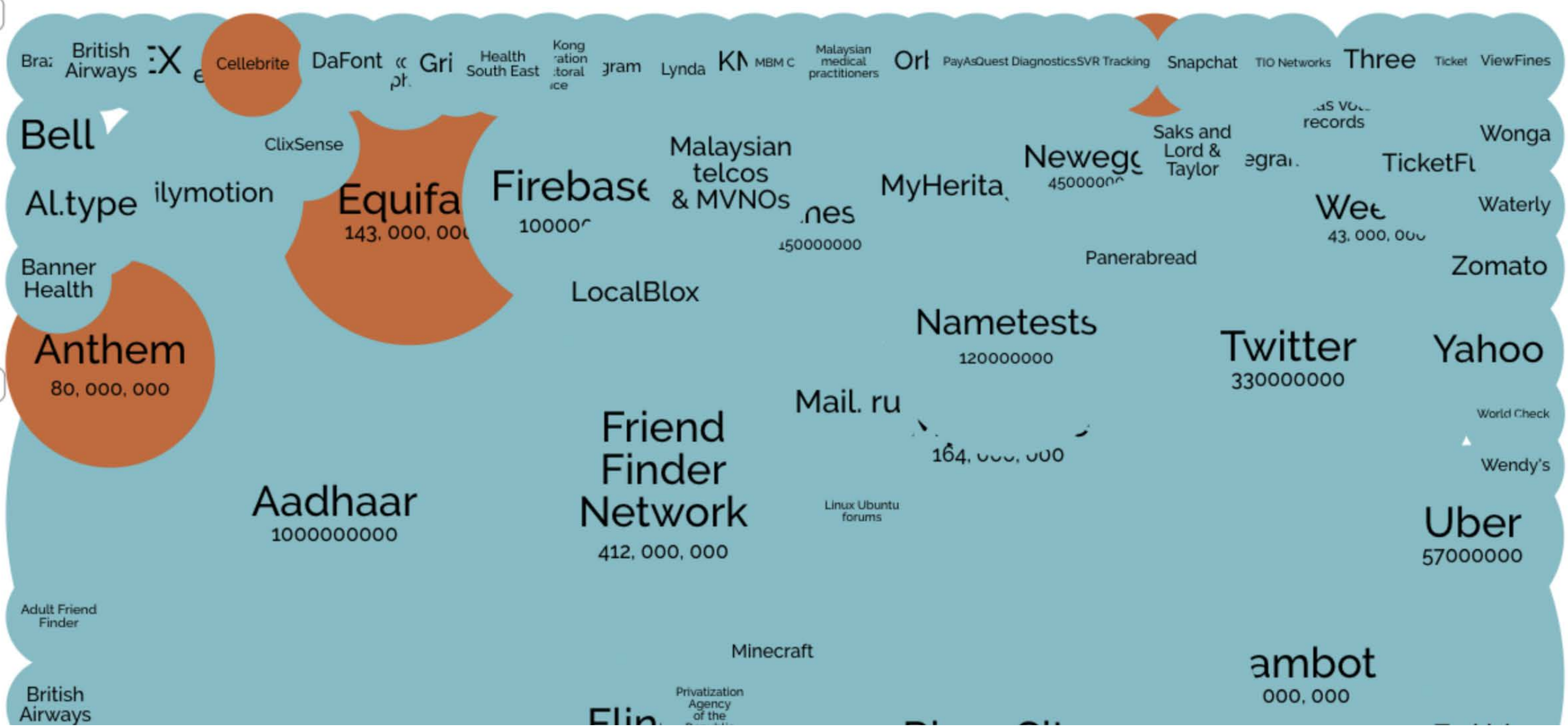
We Must Adapt

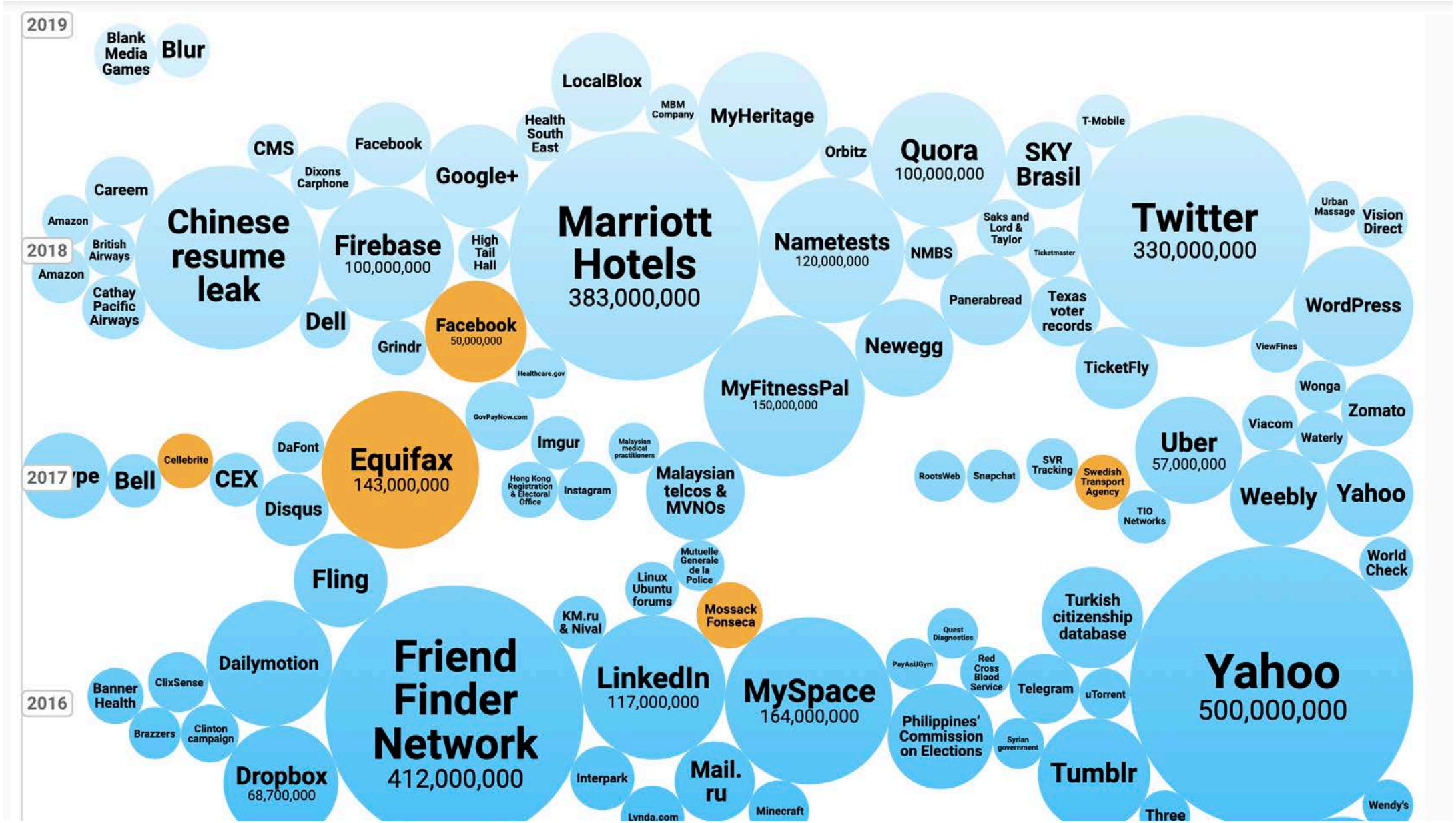


Business Challenges

Increased complexity, attack surface & gaps in visibility


latest
2015
Anthem
80. 000. 000
Carefirst
Adult Friend Finder
British Airways
Experian / T-mobile
IRS
Hacking Team
Invest Bank
Kromtech
Minecraft
Slack
MSpy
Premera
Voter Database
191 million
Verizon
AshleyMadison.com
CarPhone Warehouse
European Central Bank
JP Morgan Chase
76. 000. 000
Sanrio
US Office of Personnel Management (2nd Breach)
NASDAQ
Community Health Services
Ebay
145. 000. 000
Korea Credit Bureau
Securus Technologies
70 million
TalkTalk
Twitch.tv
VTech
Uber

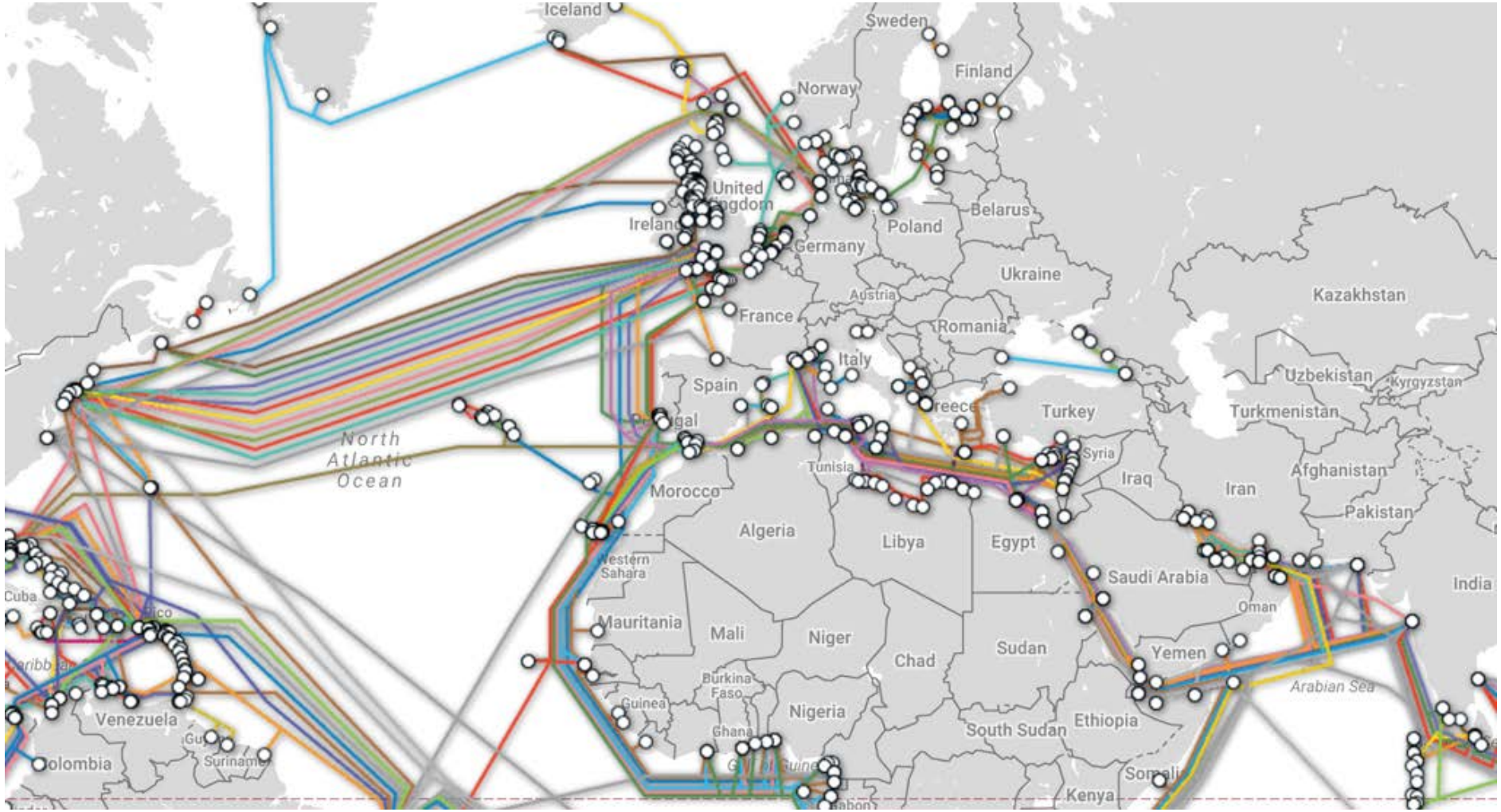

British Airways
Cellebrite
DaFont
Health South East
Lynda
MBM C
Malaysian medical practitioners
PayAsQuest Diagnostics
SVR Tracking
Snapchat
TIO Networks
Three
Ticket
ViewFines
Bell
ClixSense
Saks and Lord & Taylor
Wonga
Al.type
ilymotion
Equifa
143, 000, 000
Firebase
100000
Malaysian telcos & MVNOs
MyHerita
Newegg
45000000
records
TicketFl
Waterly
Panerabread
Zomato
Banner Health
LocalBlox
Anthem
80, 000, 000
Nametests
120000000
Twitter
330000000
Yahoo
Mail. ru
World Check
Wendy's
Friend Finder Network
412, 000, 000
Aadhaar
1000000000
Linux Ubuntu forums
Uber
57000000
Adult Friend Finder
Minecraft
ambot
000, 000
British Airways
Privatization Agency of the



Businesses Must Understand Their Supply Chain

Supply Chain

Submarine Cable Map



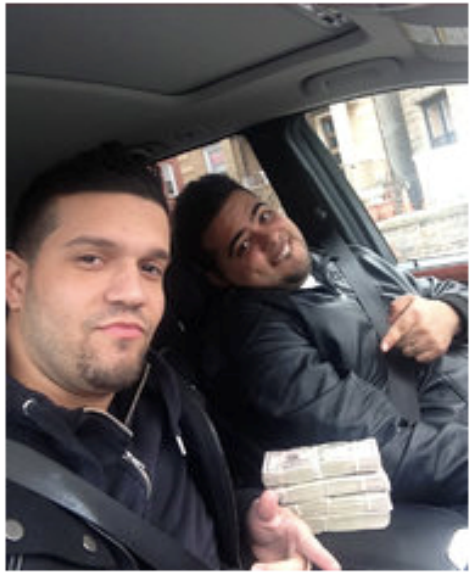
Heist

In Hours, Thieves Took $45 Million in A.T.M. Scheme

By MARC SANTORA
Published: May 9, 2013

It was a brazen bank heist, but a 21st-century version in which the criminals never wore ski masks, threatened a teller or set foot in a vault.

Enlarge This Image



United States attorney's office, Eastern District of New York

Elvis Rafael Rodriguez, left, and Emir Yasser Yeje, two of those charged in Brooklyn on Thursday, posed in March with approximately $40,000 in cash that the authorities say they were laundering.

In two precision operations that involved people in more than two dozen countries acting in close coordination and with surgical precision, thieves stole $45 million from thousands of A.T.M.'s in a matter of hours.

In New York City alone, the thieves responsible for A.T.M. withdrawals struck 2,904 machines over 10 hours starting on Feb. 19, withdrawing $2.4 million.

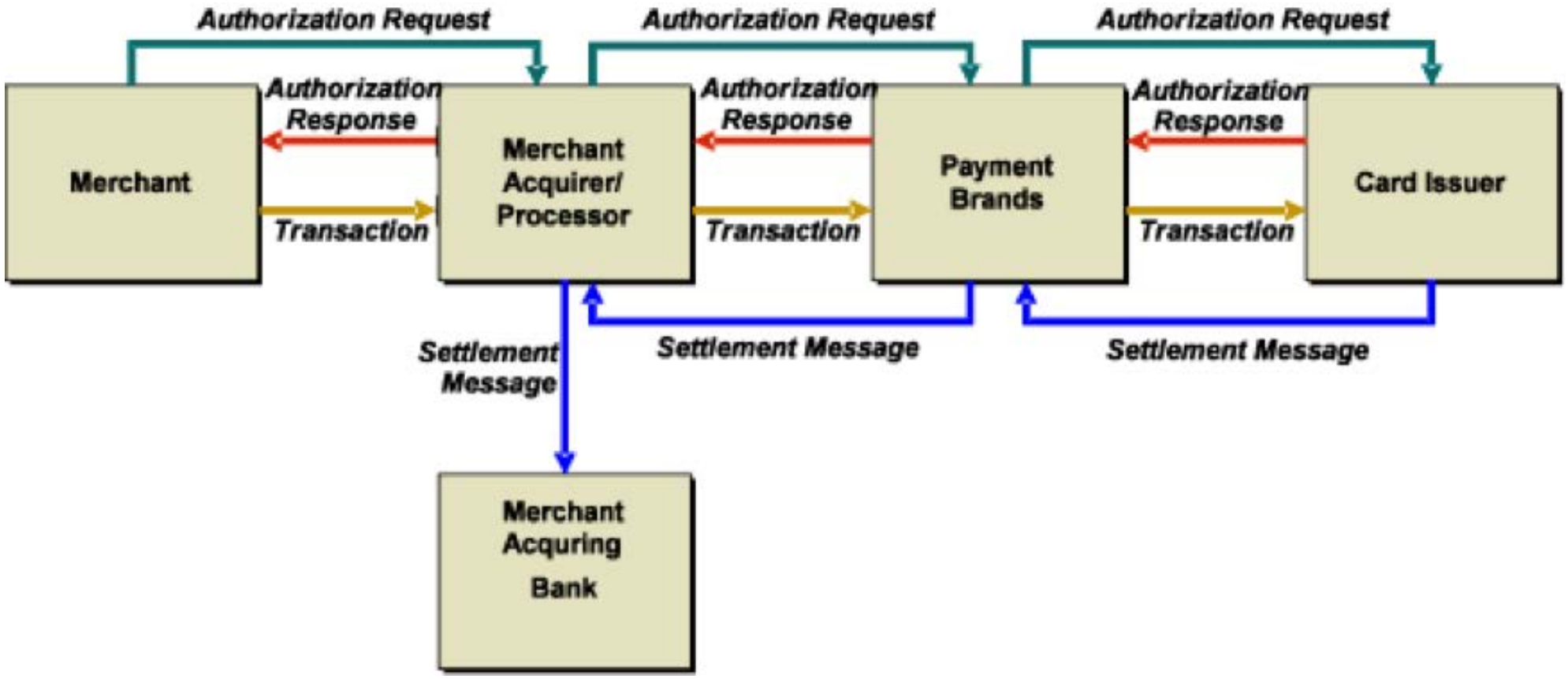
The operation included sophisticated computer experts operating in the shadowy world of Internet hacking, manipulating financial information with the stroke of a few keys, as well as common street criminals, who used that information to loot the automated teller machines.

New York


1
2
3
4
5
6
7
8
9
10


1
4:31PM- @ 2380 BROADWAY
5 WITHDRAWALS- $4,015
2
5:10PM- @ 2077 BROADWAY
3 WITHDRAWALS- $2,409
3
5:28PM- @ 1686 BROADWAY
3 WITHDRAWALS- $2,409
4
6:17PM- @ 1680 BROADWAY
3 WITHDRAWALS- $2,409
5
6:24PM- @ 1535 BROADWAY
3 WITHDRAWALS- $2,409
6
6:43PM- @ 515 SEVENTH AVE
3 WITHDRAWALS- $2,409
7
7:31PM- @ 238 EIGHTH AVE
3 WITHDRAWALS- $2,409
8
8:55PM- @ 918 THIRD AVE
3 WITHDRAWALS- $2,409
9
9:24PM- @ 991 THIRD AVE
7 WITHDRAWALS- $5,621
10
9:55PM- @ 1151 THIRD AVE
4 WITHDRAWALS- $4015

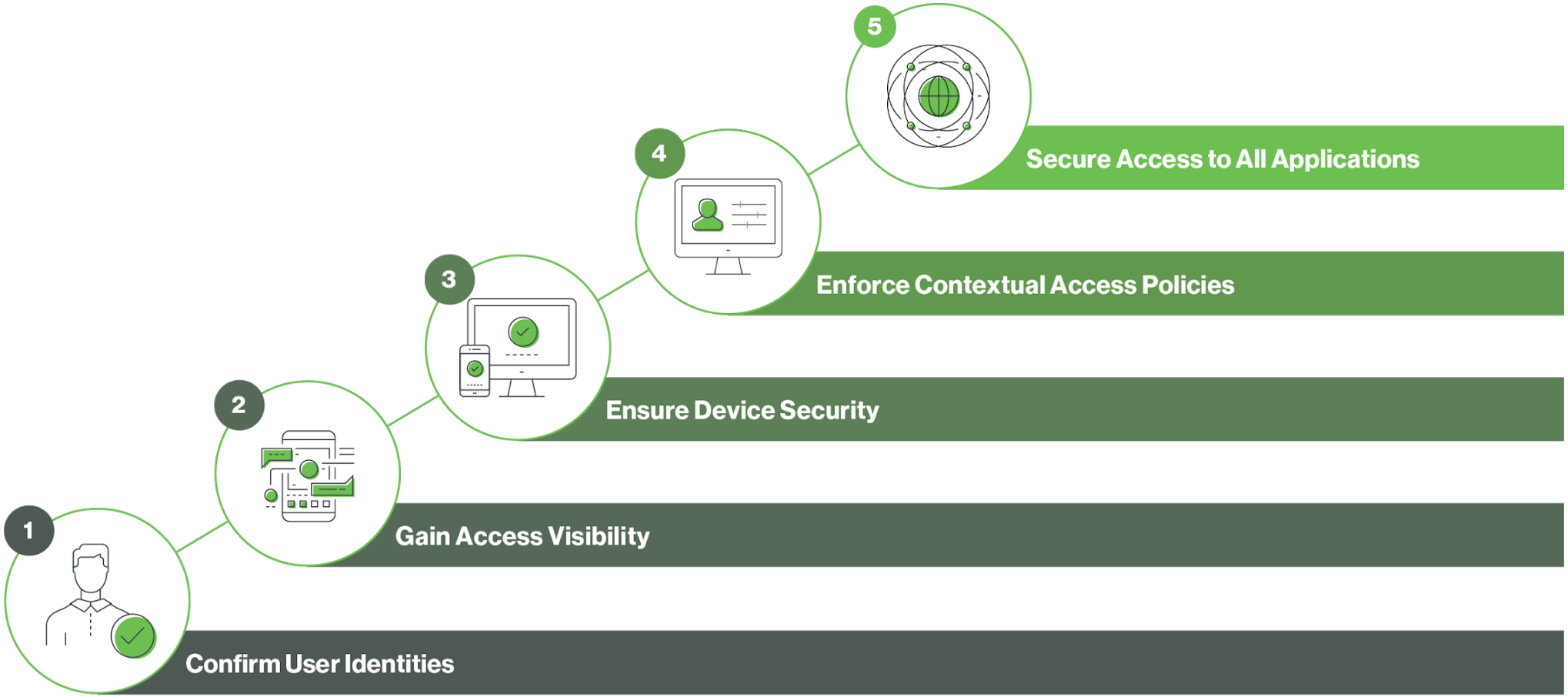
The Flow


Authorization Request
Authorization Request
Authorization Request
Authorization Response
Authorization Response
Authorization Response
Merchant
Merchant Acquirer/ Processor
Payment Brands
Card Issuer
Transaction
Transaction
Transaction
Settlement Message
Settlement Message
Settlement Message
Merchant Acquring Bank

The Penetration Test

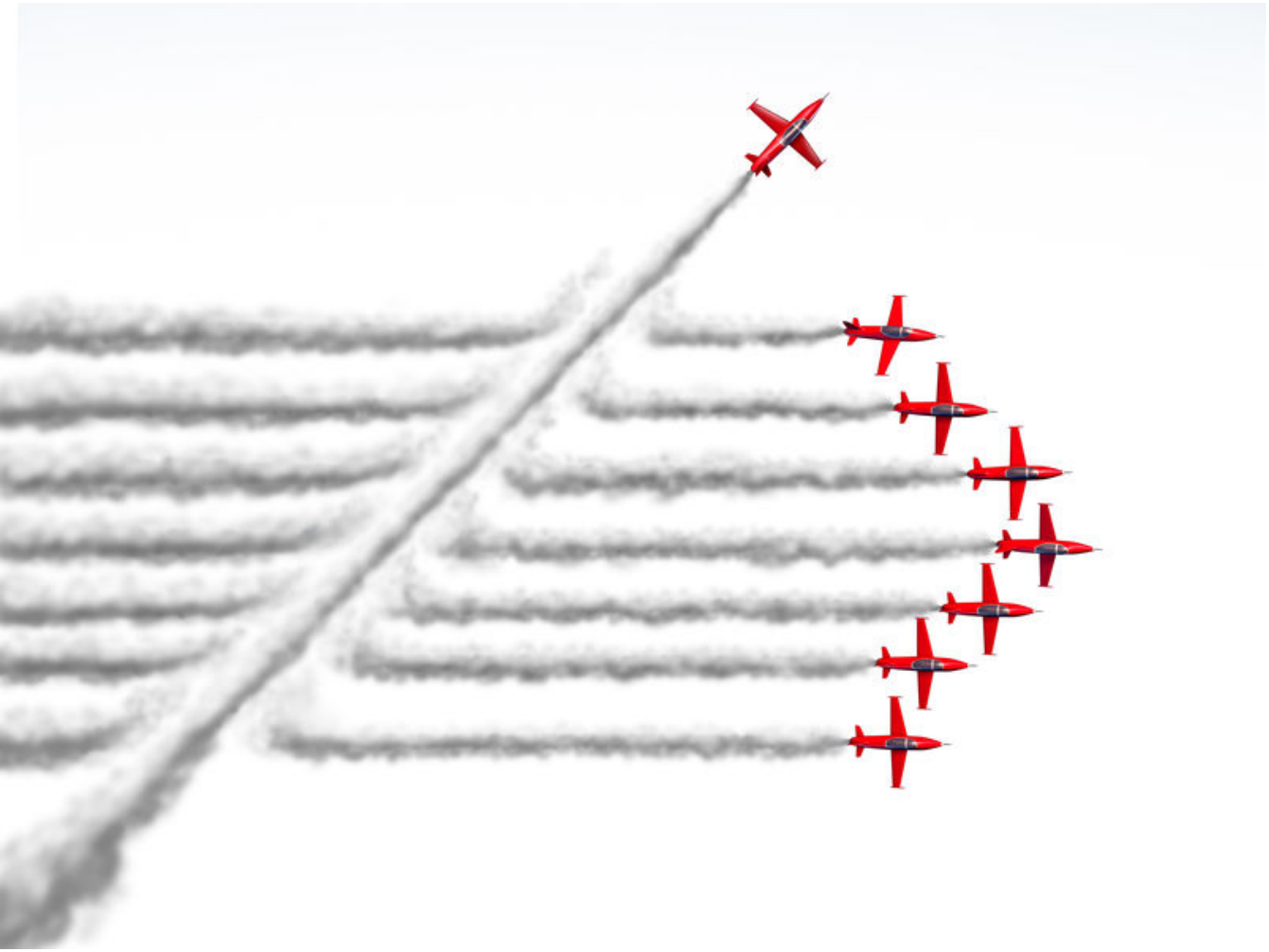
Stepping Stone to Compromising High Value Target

Strategically Think About Securing Business



Digital Transformation & SRE

Attackers Will Improvise



Return To Core Fundamentals

Apply What You Have Learned Today

- Next week you should:
  - Identify critical assets, users and applications within your organization
- In the first three months following this presentation you should:
  - Have a clearly defined risk register
  - Define appropriate controls to move towards a zero trust landscape.
- Within six months you should:
  - Begin a project to move towards a zero trust model.
  - Drive an implementation project to reduce risk in your environment.

RSAConference2019
Asia Pacific & Japan

Thanks for listening!

gattaca@cisco.com

@gattaca