DEFENDING THE EXPOSED FLANK

DIGITAL SUPPLY CHAIN SECURITY

FIRST 2017

Hi

I’m Martin McKeay

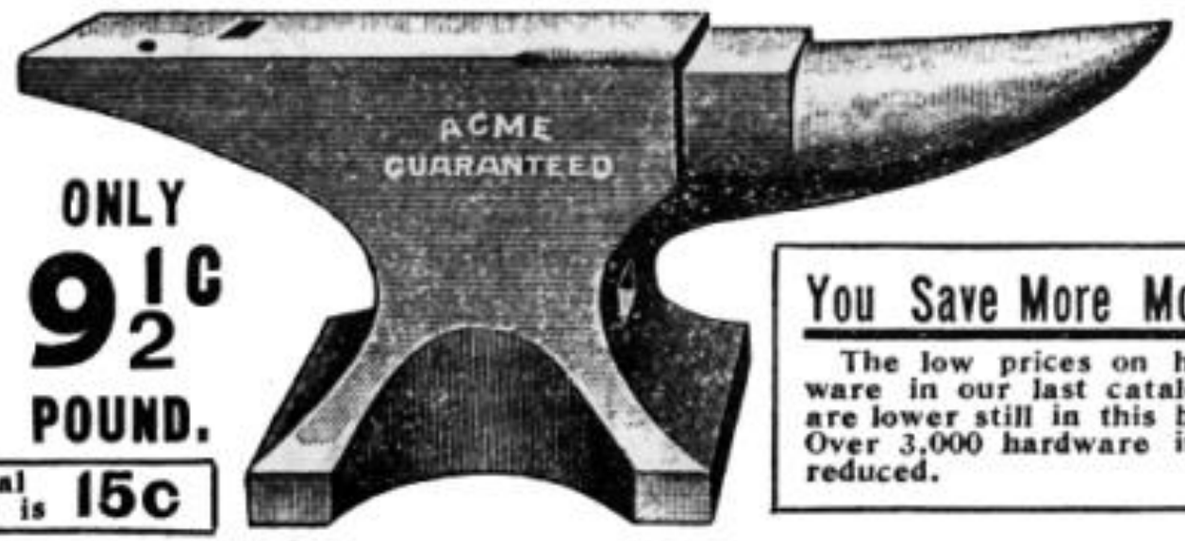
I have been in security for almost two decades

I have the scars to prove it

ACME AMERICAN WROUGHT ANVILS

THEY RING LIKE A BELL. **No anvil made, English or American, surpasses our Acme in shape, material or finish.** It is solid forged of two pieces of best wrought iron, welded at waist; face is made of one piece of tool steel, electrically welded to the body and warranted not to come loose. Base has sufficient spread to insure stability and prevent tipping; has long perfectly shaped horn and heel; face is trued and shaped by a special machine so that there are no hollow or uneven places; edges are perfectly tempered and will not chip. Hardie holes are straight and true, so you will have no trouble on account of anvil tools sticking or not setting level.

WE HAVE THE EXCLUSIVE SALE OF THE ACME. **We take the entire output of the factory that makes them,** and get them so cheap we are enabled to sell them at a lower price than others pay for anvils not as good. We sell more anvils than any concern in the United States. We could not sell so many unless they were everything we claim for them.



ONLY 9½c POUND.

Usual Price is 15c

You Save More Money

The low prices on hardware in our last catalogue are lower still in this book. Over 3,000 hardware items reduced.

I am the Sr. Editor of the State of the Internet/Security report

Now, I work for 

This isn’t a vendor pitch

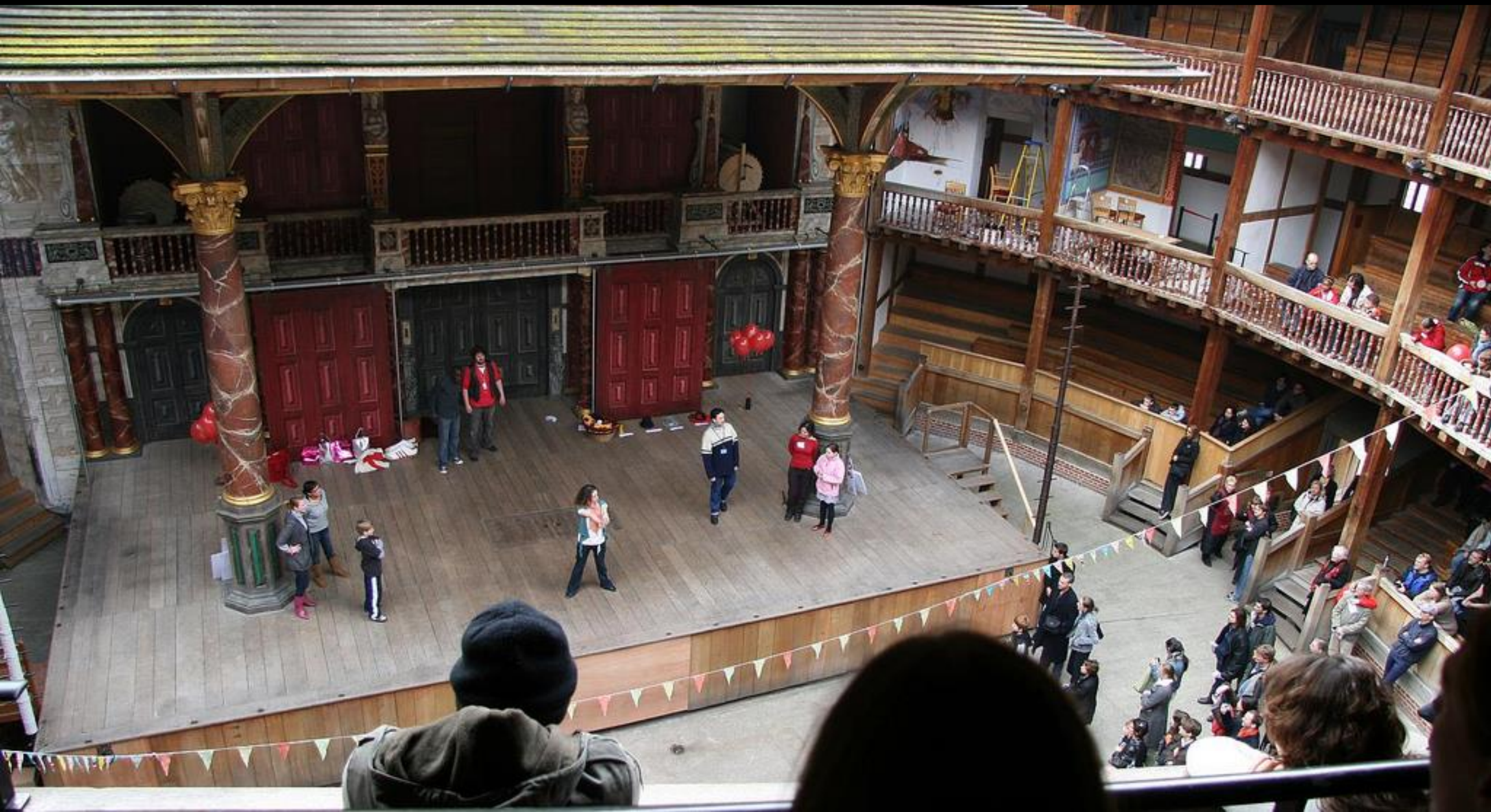

HONEST

I’m here to talk about the exposed flank

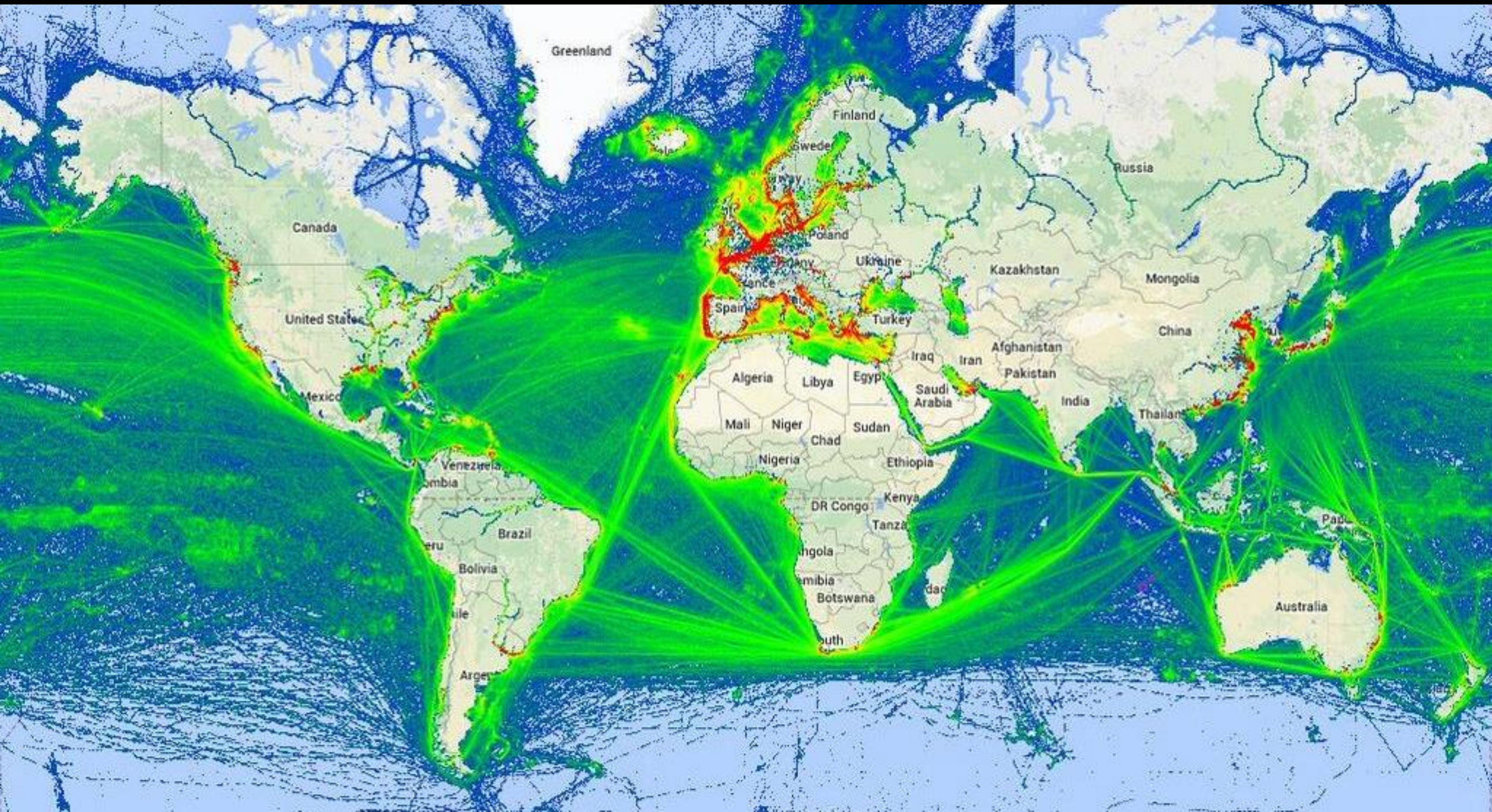
Digital Supply Chain Security

ACT 1

MEANING



PHYSICAL SUPPLY CHAIN



DIGITAL SUPPLY CHAIN

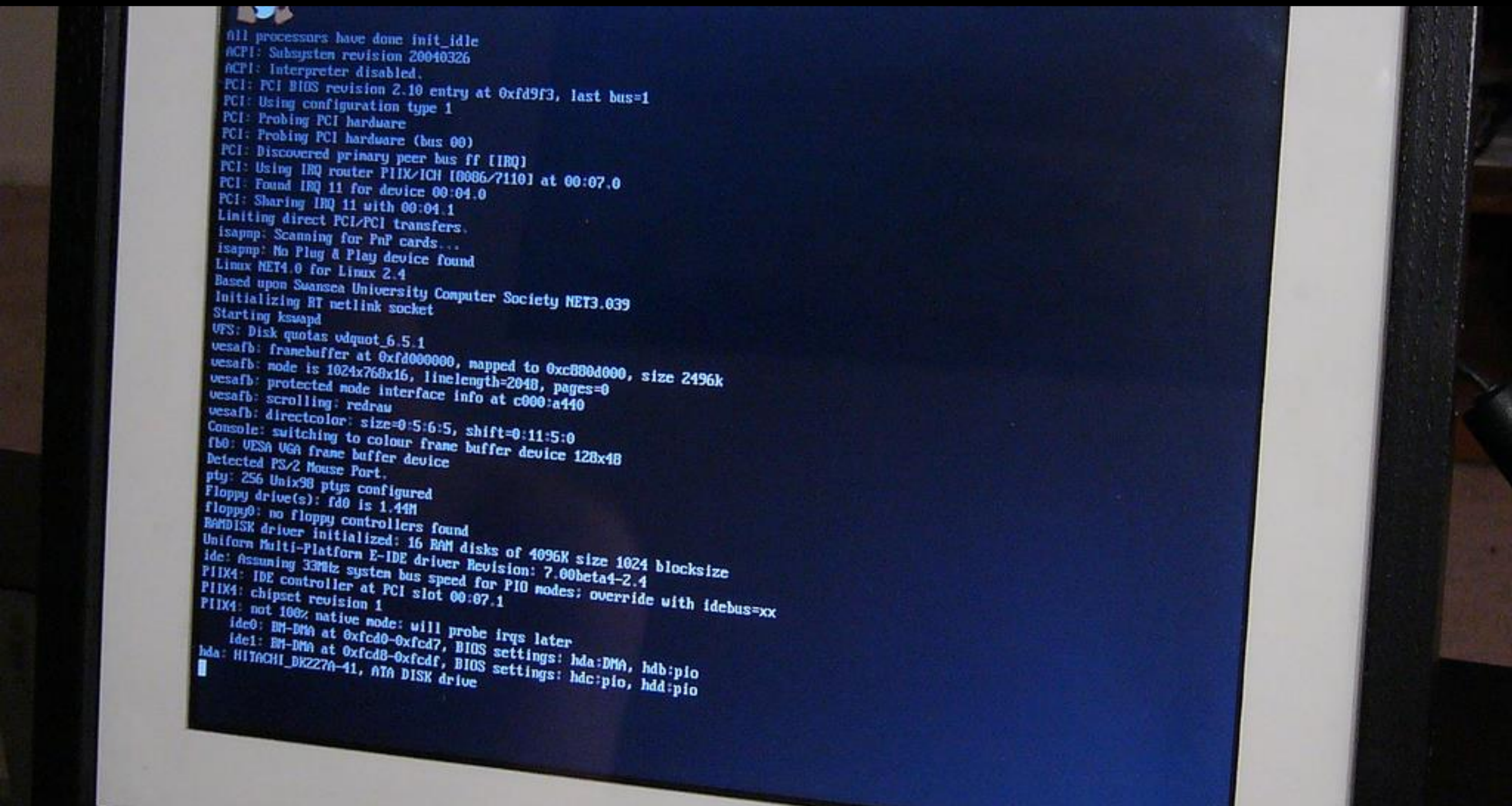
WHAT DO I MEAN?

- Supply chain in this perspective is the managing of the internal components of an organization.
- The security to ensure the integrity of the information technology systems.
- Addressing security at all points in the workflow so that attackers may not openly compromise systems.
- Attackers might have been focused on stealing trucks historically, now they’re after your code.

WHO ELSE IS TALKING ABOUT THIS?

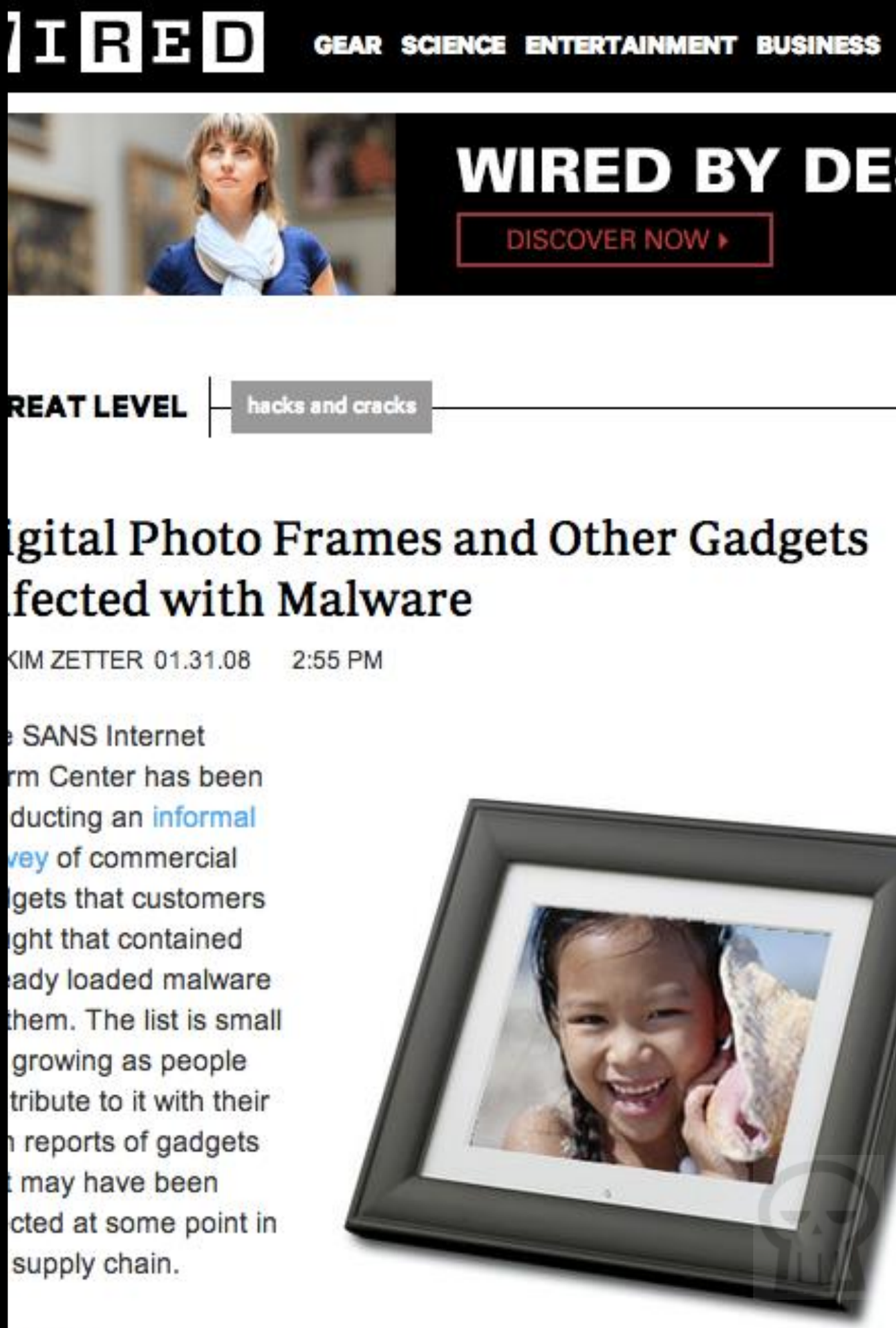
EXAMPLE OF A DIGITAL PICTURE FRAME OR USB DRIVE

HOW DID MY WIDGET GET HERE?



MALWARE IN THE PIPELINE...

- Supply chain issues with regard to Information Technology began to show themselves early on.



OR WORSE...

POOR SECURITY IN CODE

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x48\x52\x41", 5);              // root     xmhdipc
add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root     default
add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root     juantech
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin    password
add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                          // root     root
add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                      // root     12345
add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                          // user     user
add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                      // admin    (none)
add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                          // root     pass
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);  // admin    admin1234
```

THE GROUND FLOOR

- The focus in supply chain security has historically been towards enhancing the physical security of the supply chain logistics.
- Lack of concentration on the information technology/security
- Greater move to decentralized information technology solutions with global scale
- Information technology and the supply chain

WHO CARES?

- Who is taking the time to work on the problem?
- Organization that on supply chain include:
- World Customs Organization (WCO), Customs Trade Partnership against Terrorism (C-TPAT), Container Security Initiative(CSI) from the US Customs and Border Protection and the Global Security Initiative from DHS.
- ISO/PAS 28000 “Specification for security management systems for the supply chain”

MAGINOT LINE

- There is a concerted effort to secure physical side of logistics.
- IT solutions as they relate to supply chain have typically lacked the same focus.
- So why should this be of concern?
- Well...

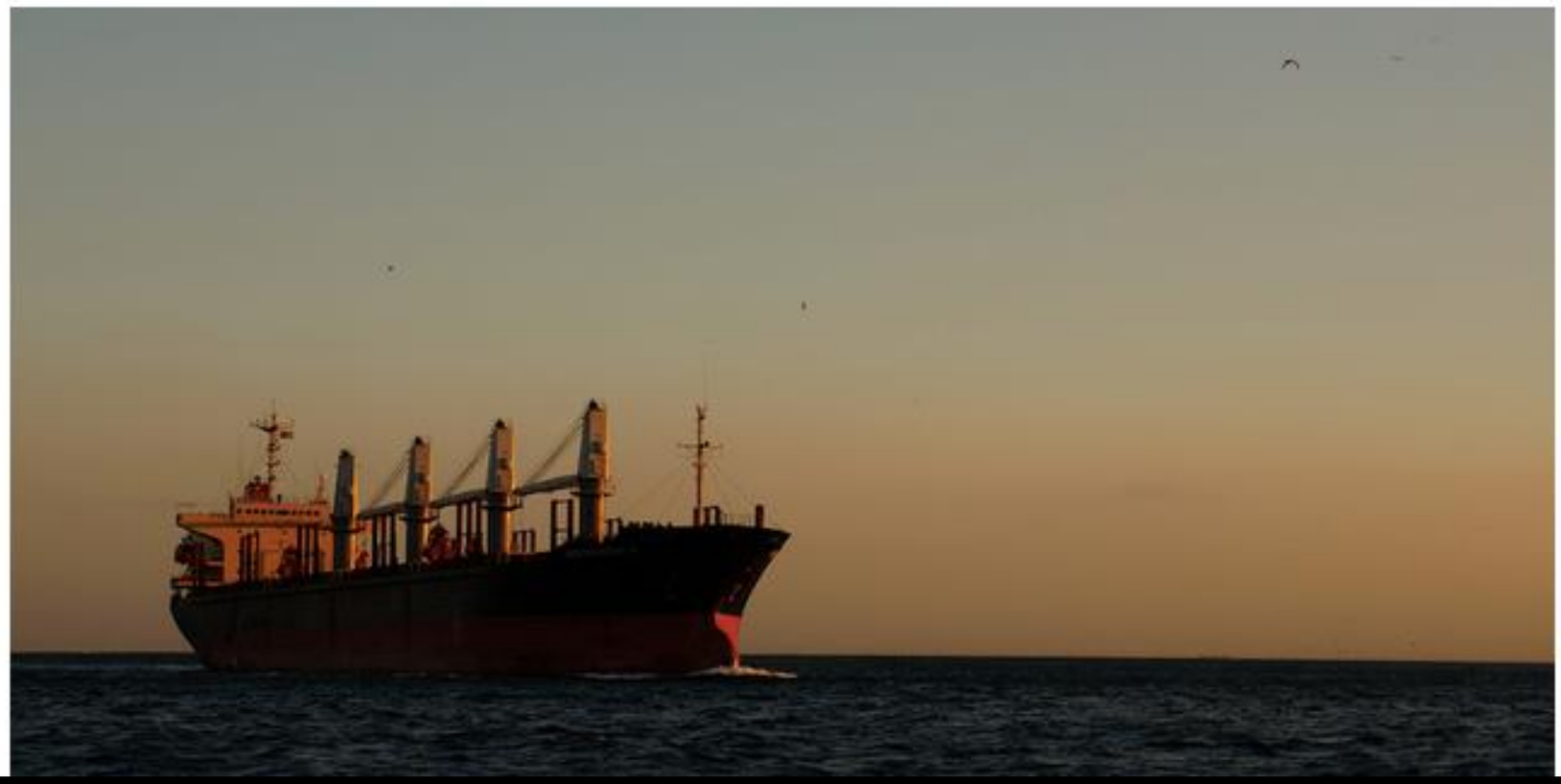
CASE IN POINT...

NEWS

An Iranian Oil Tanker Hacked Its Own Tracking System To Avoid Detection

ADAM CLARK ESTES *31 OCTOBER 2013 3:30 PM*

Share 16 Discuss 10 Bookmark



WHAT COULD GO WRONG?

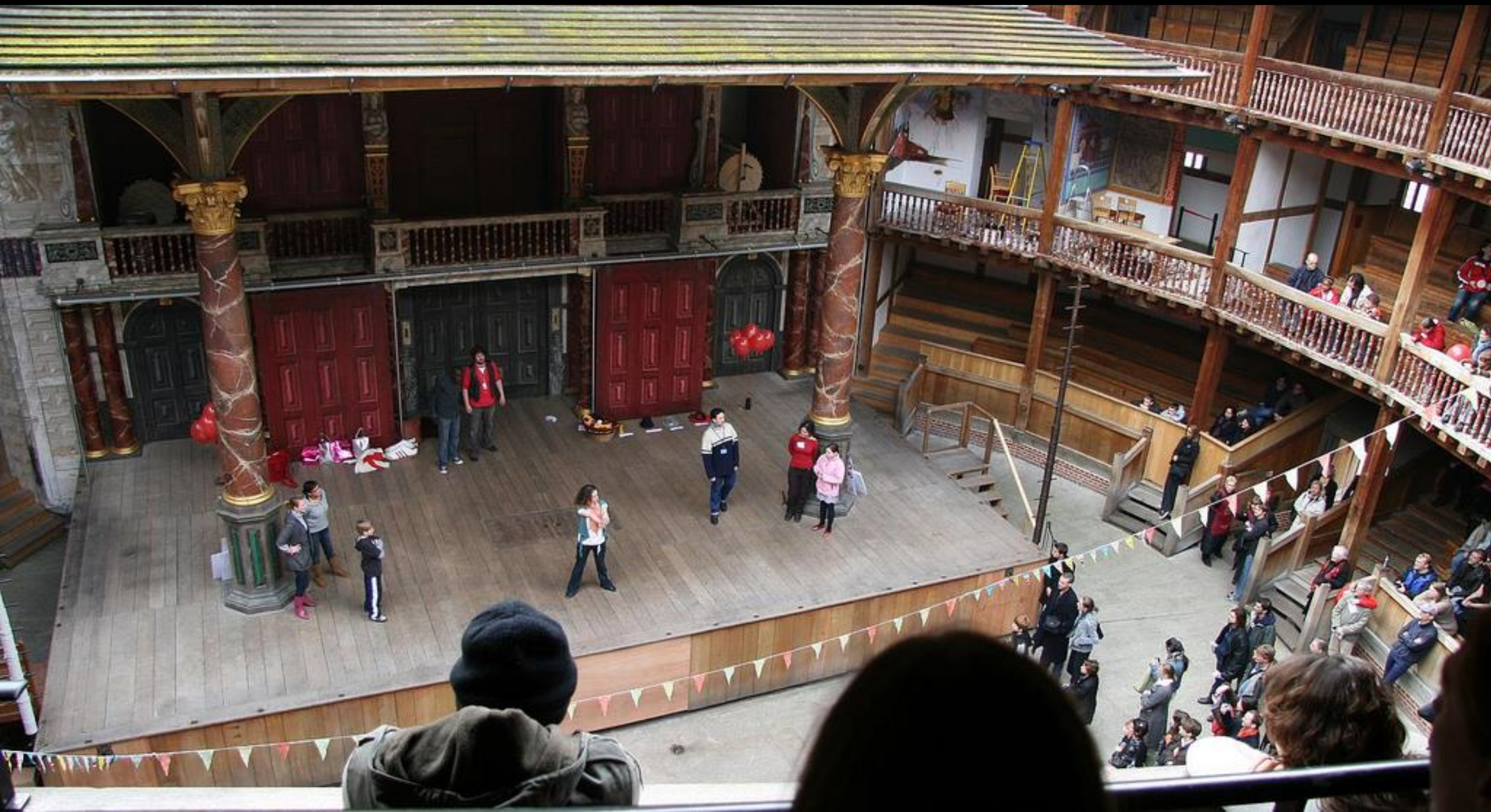
Pirates hacked shipping company to steal info for efficient hijackings

07 MAR 2016 2

Data loss, Security threats, Vulnerability

WAR STORIES AND SUCH

ACT II



GLOBAL, LEGAL, COMPLEXITY, HUMAN...

CHALLENGES & COMPLICATIONS

CHALLENGES

- As we have more an more products delivered to us faster and cheaper the scale of operations has gone to go global scale.
- What are some impacts of this move?
  - Outsourced help desk
  - Offshore development centres
  - Partner networks

GEOPOLITICAL

LEGAL ISSUES

- Legal issues are now global ones as supply chain expands across the globe.
- How do laws affect the production supply chain?
- Is there a lack of enforcement of said laws?
- Are you even legally able to be operating in the country?
- Ignorance of the law is no defense.

ATM, FAVORITE OF NE'ER DO WELLS

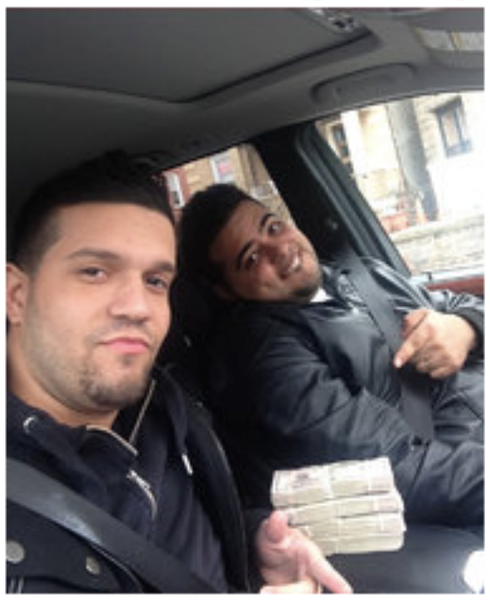
ANOTHER LEGAL ISSUE EXAMPLE, ATM FRAUD

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

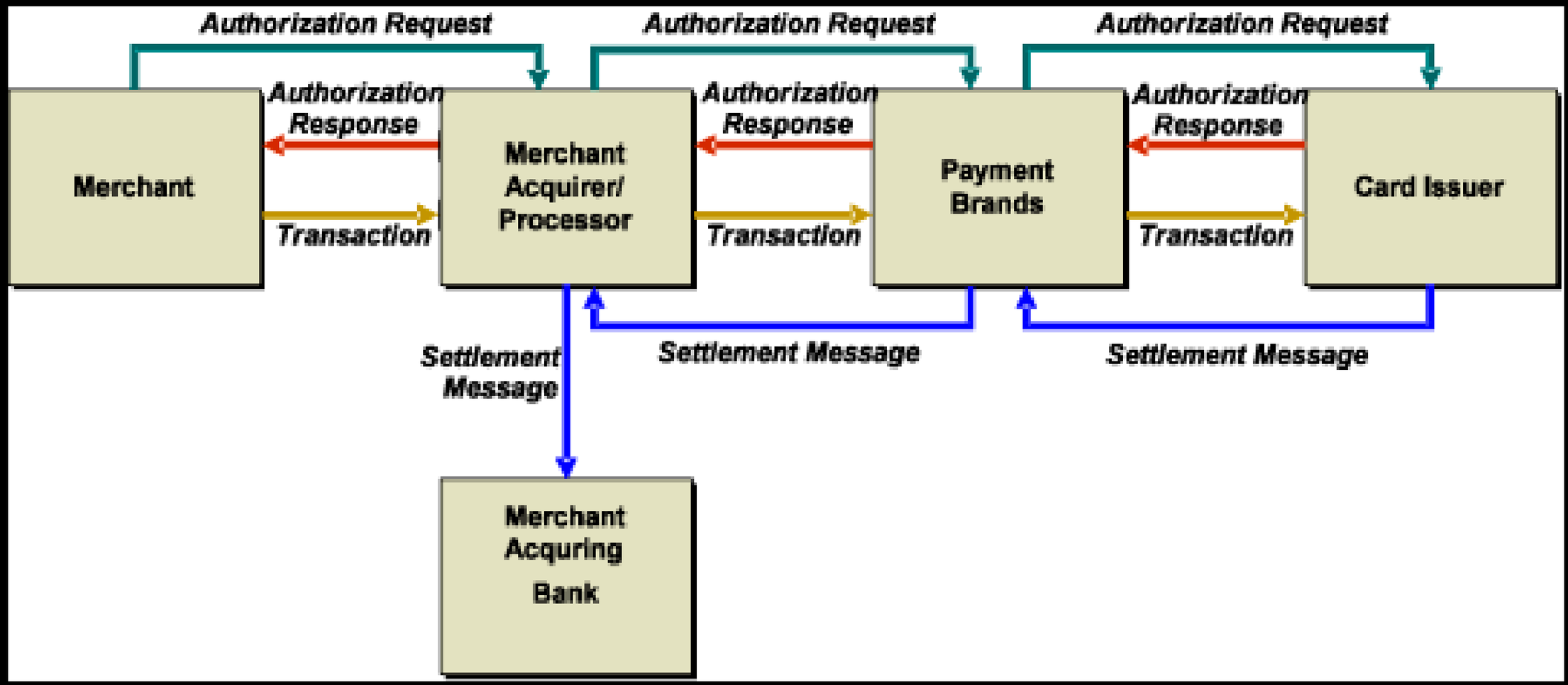
Elvis Rafael Rodriguez, left, and Emir Yasser Yeje, two of those charged in Brooklyn on Thursday, posed in March with approximately $40,000 in cash that the authorities say they were laundering.

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.

THE FLOW


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

WHAT WENT WRONG?

- Vulnerable financial institutions
- Credit card processor was breached on two occasions
- Withdrawal limits removed on prepaid debit cards
- Cashing teams: 36,000 transactions and withdrew about $40 million from machines in the various countries in about 10 hours

INTELLECTUAL PROPERTY

- We have all read about the APT problems.
- Concerted efforts to purloin Intellectual Property. (Source Code, Process, Secret Sauce)
- Using tools like Perforce and Git (as examples) partners often want access to source code.
- Too often they get this access as a “business decision” which is your organization’s secret sauce.

SOURCE CODE ISSUES

Security Advisories Relating to Symantec Products - Symantec Reporting Server Improper URL Handling Exposure

SYM09-008

April 28, 2009

Revision History
None

Risk Impact
Low

Remote Access	No
Local Access	Yes
Authentication Required	No
Exploit available	No

Overview

The login web page in some versions of Symantec Reporting Server contains a URL handling error which could potentially allow an attacker to launch a phishing attack.

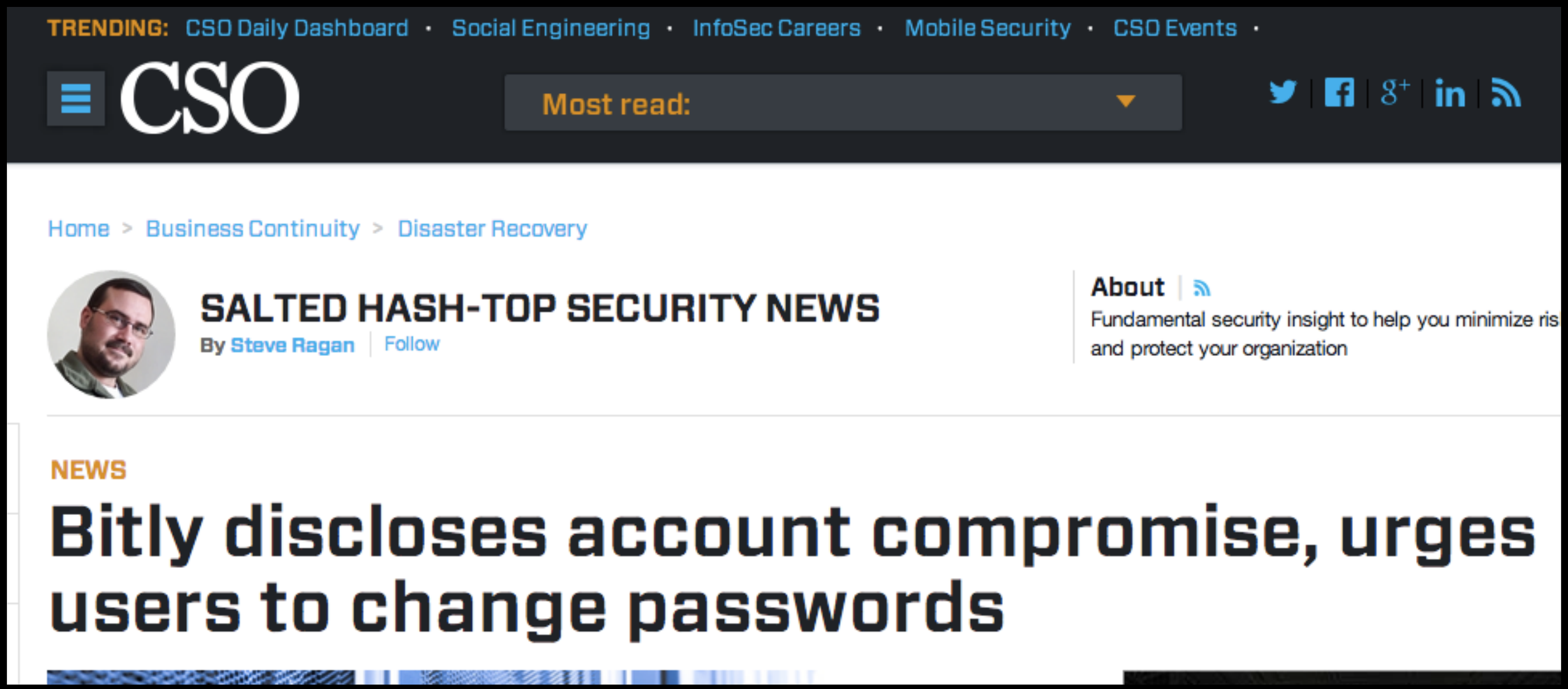
Affected Products

Product	Affected Version	Solution
Symantec AntiVirus Corporate Edition	10.1 MR7 and earlier	Update to 10.1 MR8 or later
	10.2 MR1 and earlier	Update to 10.2 MR2 or later
Symantec Client Security	3.1 MR7 and earlier	Update to 3.1 MR8 or later
Symantec Endpoint Protection	11.0 MR1 and earlier	Update to 11.0 MR2 or later

Unaffected Products

Product	Version

...AND SO ON


TRENDING: CSO Daily Dashboard · Social Engineering · InfoSec Careers · Mobile Security · CSO Events ·
CSO
Most read:
Home > Business Continuity > Disaster Recovery
SALTED HASH-TOP SECURITY NEWS
By Steve Ragan | Follow
About
Fundamental security insight to help you minimize ris
and protect your organization
NEWS
Bitly discloses account compromise, urges users to change passwords

PARTNER NETWORKS

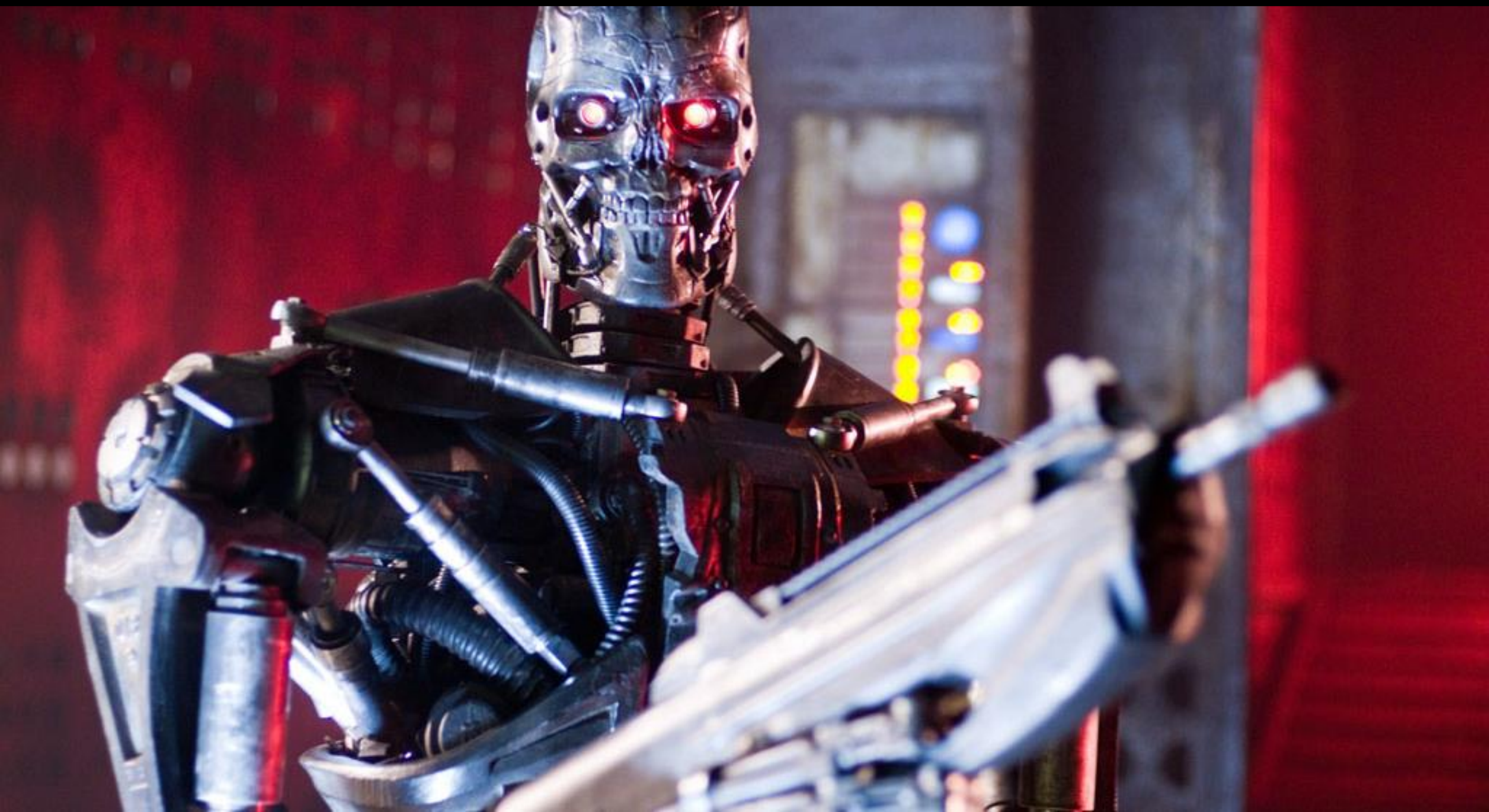
- Many manufacturing companies build and maintain interconnected networks
- The “I have a firewall so I’m OK” mentality should be shelved.
- Do you check your third party connections?
- Trust But (Test and) Verify

HARDWARE TROJANS

MORE RECENTLY...

BATTLEFIELD ROBOTS

YIPES!



OH...RIGHT

WAIT WHAT?

THIS IS REAL

DOD officials say autonomous killing machines deserve a look

While military requires person in loop, robots might decide when to shoot in future.

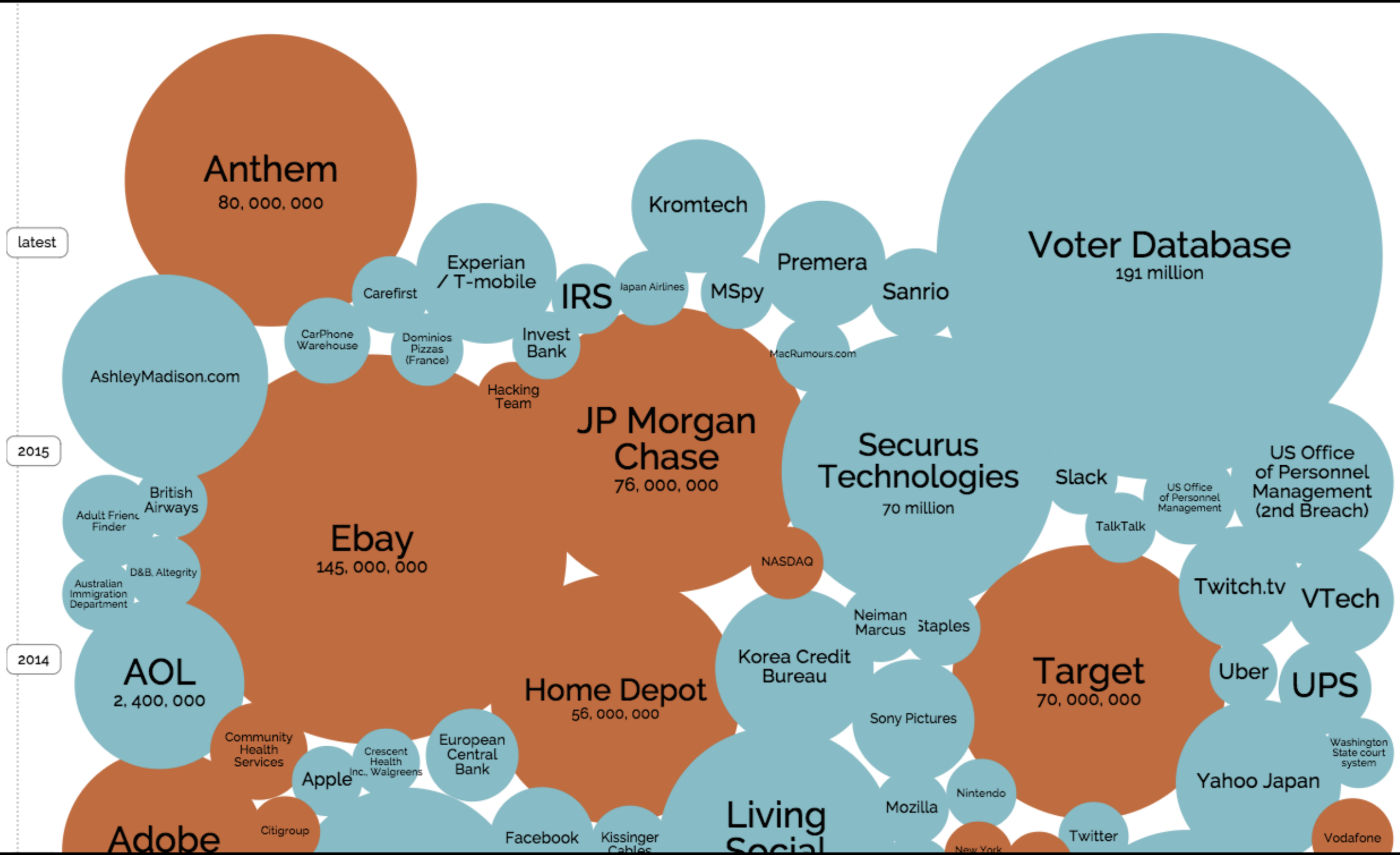
by **Sean Gallagher** - Mar 4, 2016 7:14pm CET

THE TECHNOLOGY

ISN'T THERE YET

A Google self-driving car has finally caused an accident

Updated by Timothy B. Lee on February 29, 2016, 6:20 p.m. ET ✉ *tim@vox.com*


latest
2015
2014
Anthem
80, 000, 000
AshleyMadison.com
British Airways
Adult Friend Finder
D&B, Altegrity
Australian Immigration Department
AOL
2, 400, 000
Carefirst
Experian / T-mobile
CarPhone Warehouse
Dominios Pizzas (France)
IRS
Invest Bank
Hacking Team
Kromtech
Japan Airlines
MSpy
Premera
Sanrio
MacRumours.com
Voter Database
191 million
JP Morgan Chase
76, 000, 000
Ebay
145, 000, 000
Home Depot
56, 000, 000
Community Health Services
Apple
Crescent Health Inc., Walgreens
European Central Bank
Citigroup
Facebook
Kissinger Cables
Adobe
NASDAQ
Neiman Marcus
Staples
Korea Credit Bureau
Sony Pictures
Living Social
Mozilla
Nintendo
Twitter
New York
Securus Technologies
70 million
Slack
US Office of Personnel Management
TalkTalk
US Office of Personnel Management (2nd Breach)
Twitch.tv
VTech
Target
70, 000, 000
Uber
UPS
Yahoo Japan
Washington State court system
Vodafone

Brazzers

Minecraft

Mossack Fonseca

National Childbirth Trust

Banner Health

Mutuelle Generale de la Police

MySpace
164. 000. 0

Slack

TalkTalk

Code.org

Hacking Team

Securus Technologies
70. 000. 000

Carefirst

MSpy

Voter Databas
191. 000. 000

Sanrio

Staples

Ebay
145. 000. 0

JP Mor
Chase
76. 000. 000

NASDAQ

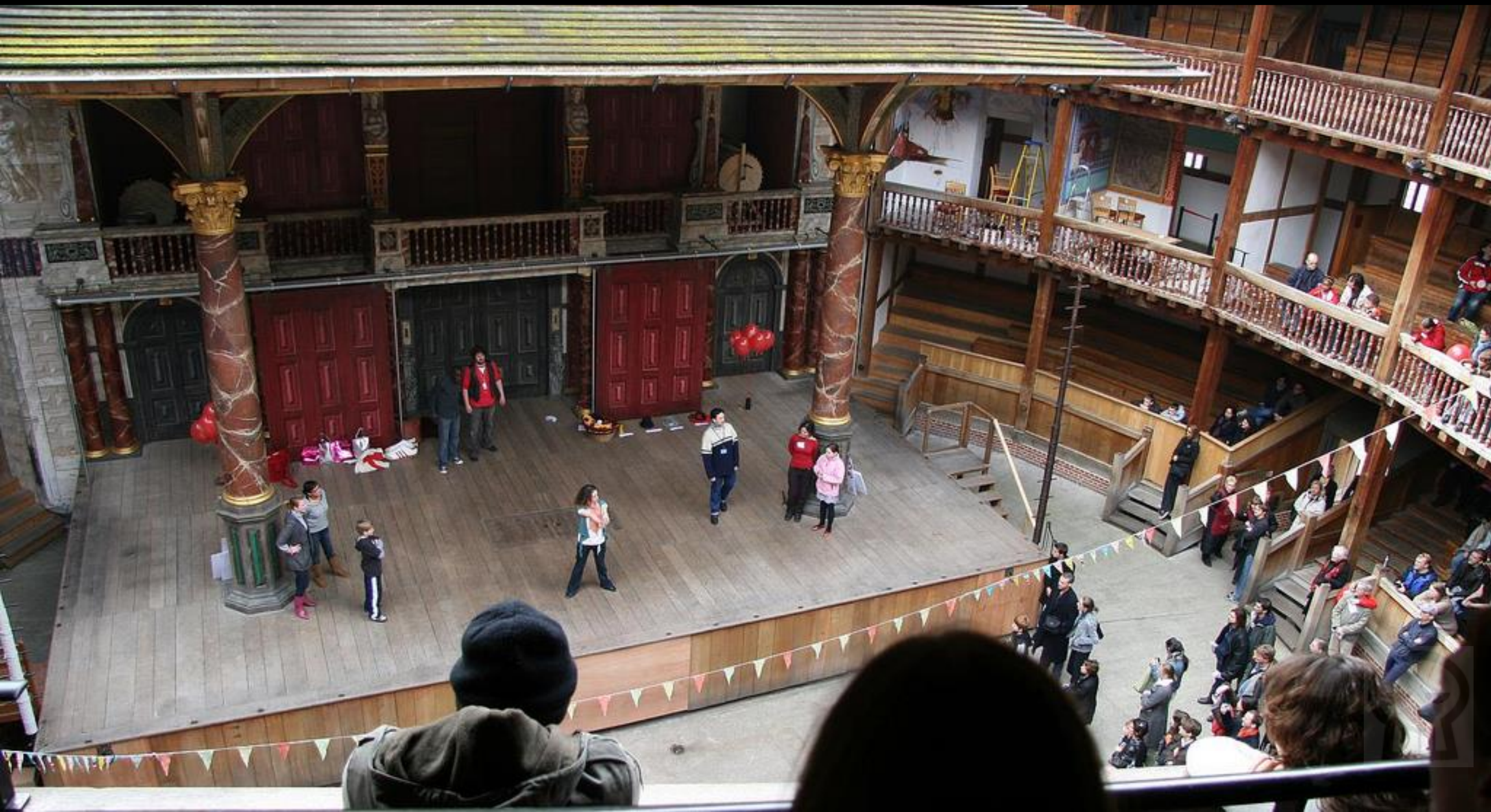
New York Taxis

Yahoo
500000000

Drupal

WHERE TO FROM HERE?

ACT III



GO BEYOND COMPLIANCE

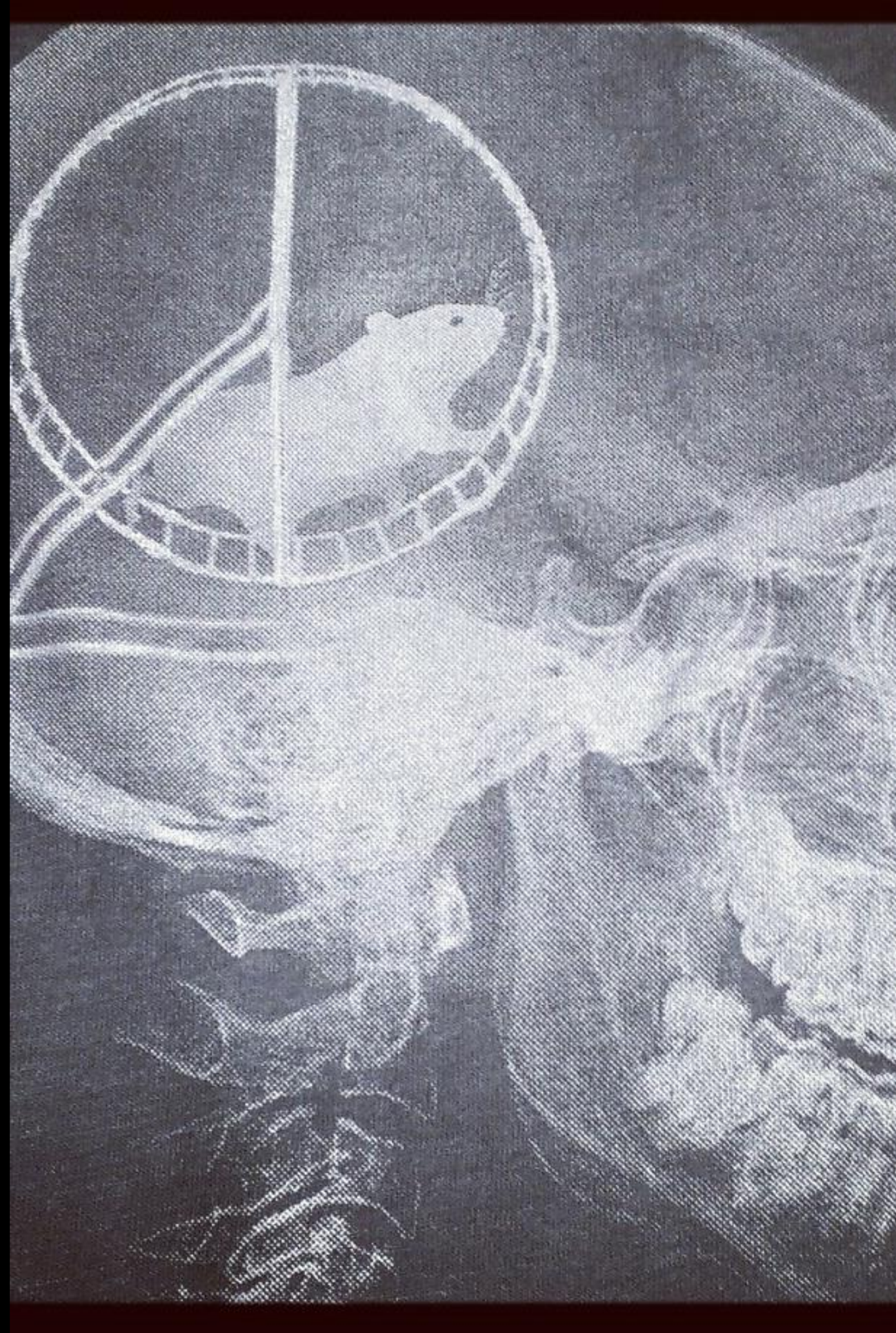
- Compliance regimes are to address the BARE MINIMUM

OFF SHORE DEVELOPMENT

- Greater diligence is required when signing a contract
- The lowest bid is not always the best choice
- Ensure that you’re development partner adheres to your security requirements
- Make sure that they do not have offices in restricted countries
- Software liability?

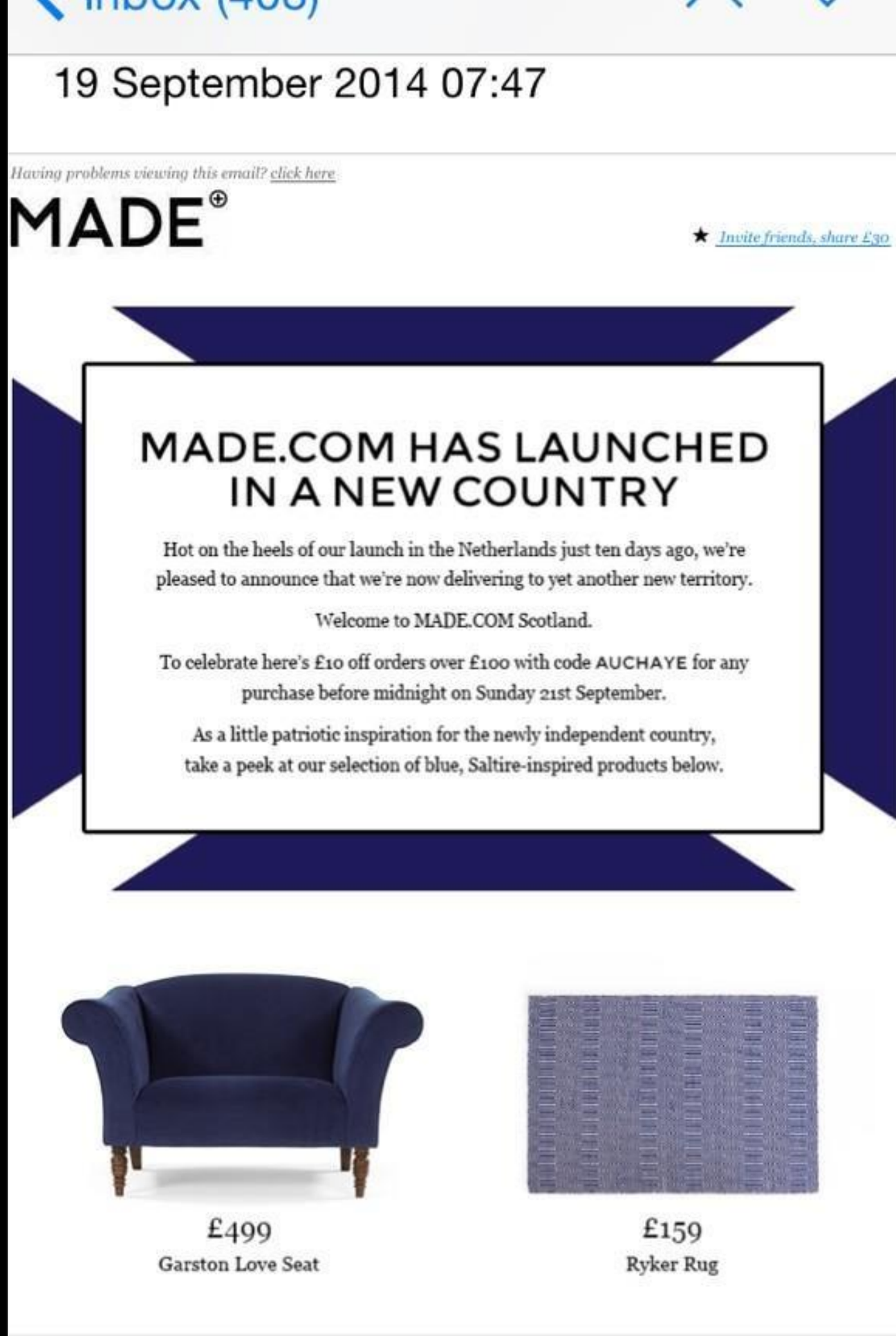
HAMSTER WHEEL OF PAIN

- How do we get off this wheel of security issues?
- We need to be able to reproduce good results



DEFINED REPEATABLE PROCESSES

- There needs to be a concentration on defined repeatable processes
- Too often companies treat third party connections as one offs. (not for all of course)
- Not having a defined on-boarding process for partners can result in unintended consequences.



THE BUDGET BATTLE

- The hardest battle I have ever fought has been for budget
- You need to make a strong case that articulates the risks to the business in terms that the business can understand.
- Avoid the fear, uncertainty and doubt if at all possible.

INTERNAL APPLICATIONS

- Conduct code reviews. Go beyond unit tests.
- Hire third party companies to review code.
- Keep documentation current

INFRASTRUCTURE, DNS & WEB APPLICATIONS

- You have limited resources
- Concentrate on the items that are important in your supply chain
- Have a trusted partner

BUILD TO FAIL

- As with any IT implementation failure will come
- Make your applications/infrastructure resilient
- Don’t build for five nines
- Build to fail

BAMBOO ANALOGY

- Supply chain has many points that can be exploited along the way
- It is important to have a supply chain that can adapt

Thank you for taking the time to listen to me!

Questions?
Thanks

Martin McKeay
@mckeay

mmckeay@akamai.com