DEFENDING THE EXPOSED FLANK

DIGITAL SUPPLY CHAIN SECURITY

BSides Ljubljana 2016

Hi

I’m Dave Lewis

I was a defender for almost two decades

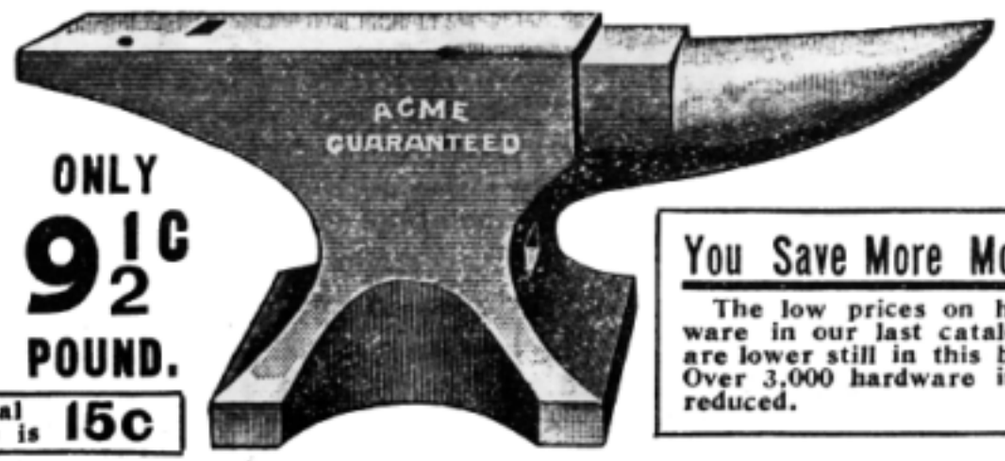
CV: ca.linkedin.com/in/gattaca/

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.

WHAT HAVE I DONE LATELY?

- Contributor at Forbes
- Writer for CSO Online
- Advisory board for Sector Security Conference
- Co-Founder of OpenCERT Canada
- Founder of liquidmatrix.org
- Board of Directors for (ISC)2

Now, I work for 

SAFE TO SAY...

I'M PRETTY HAPPY ABOUT THAT

This isn’t a vendor pitch


HONEST

I’m here to talk about the exposed flank

Digital Supply Chain Security

LEVEL SETTING

- I have merely lived it for the last 20 years or so.
- I’m here to share my perspectives and lessons learned.
- A collection of my experiences that I hope may provide you with value and actionable items.

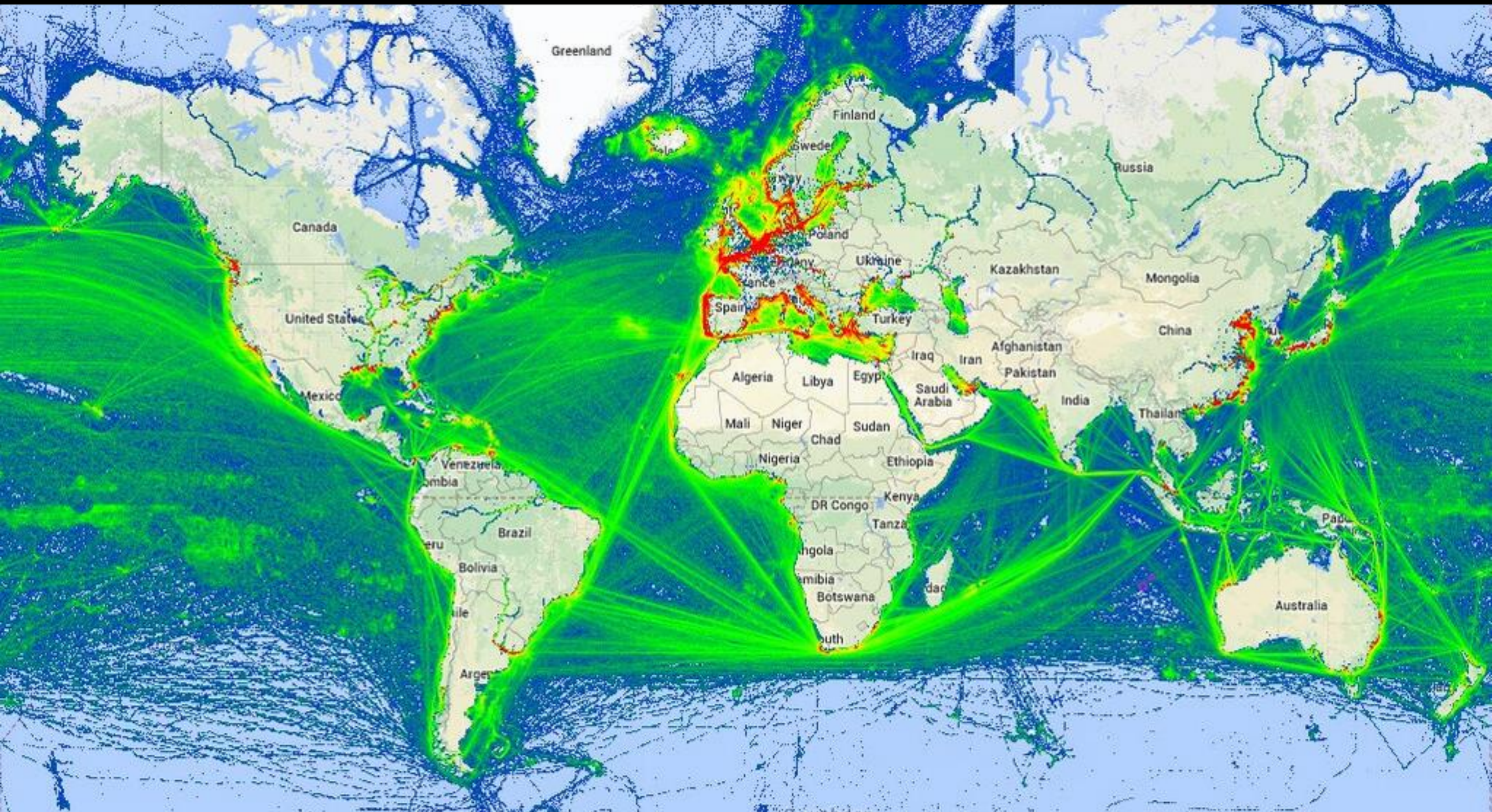
ACT 1

MEANING

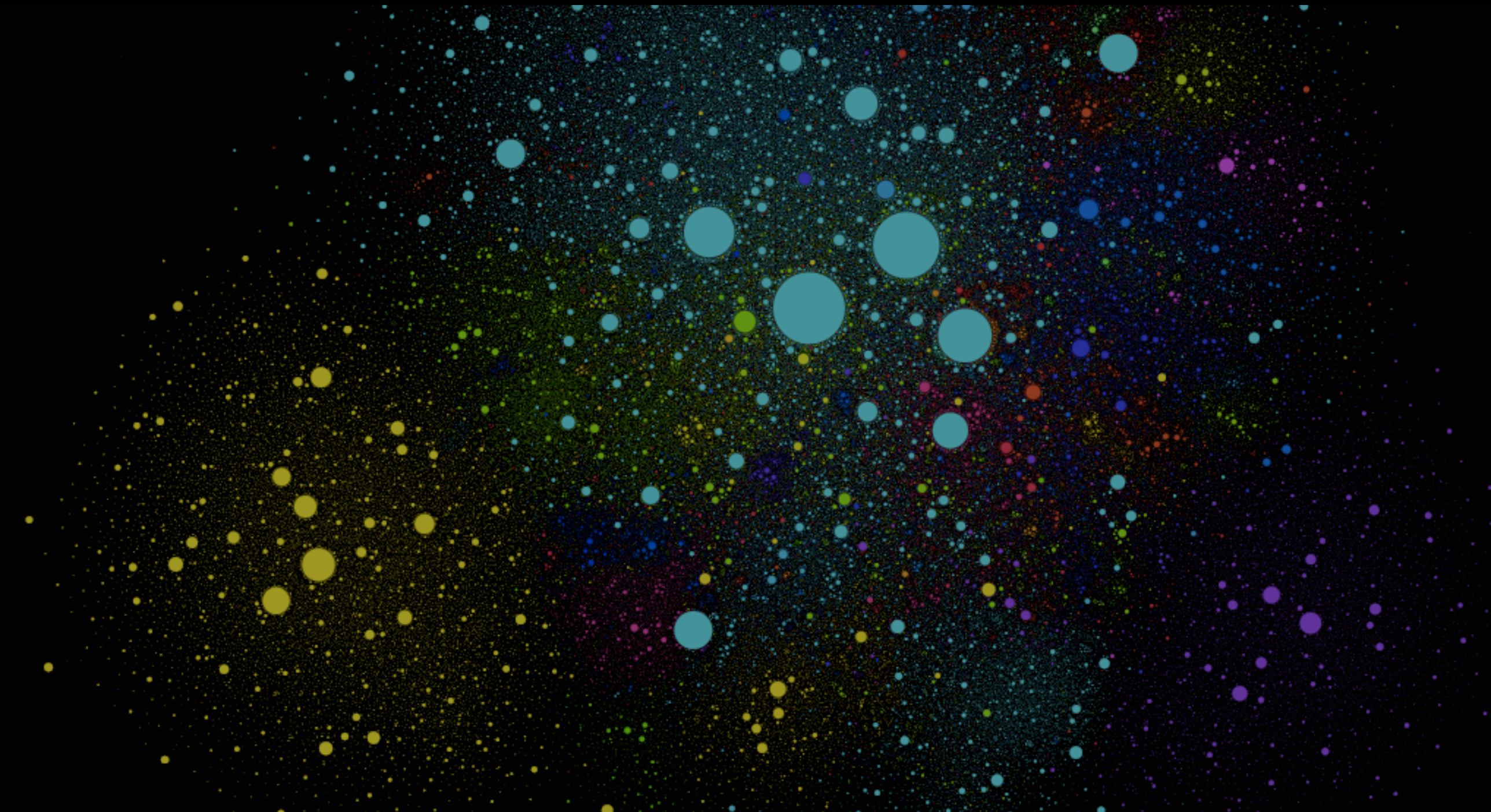
WHY I'M INTERESTED

- When I was young I would hear tales of my grandfathers crossing the Atlantic during WWII.
- One grandfather was delivering goods in the merchant marine.
- One grandfather was defending the convoys in the Canadian Navy.
- I learned the perspectives of the attackers and the defenders and the associated cost.
- Thus my fascination with supply chain security began.

PHYSICAL SUPPLY CHAIN



DIGITAL SUPPLY CHAIN



ONE & A HALF YEARS LATER...

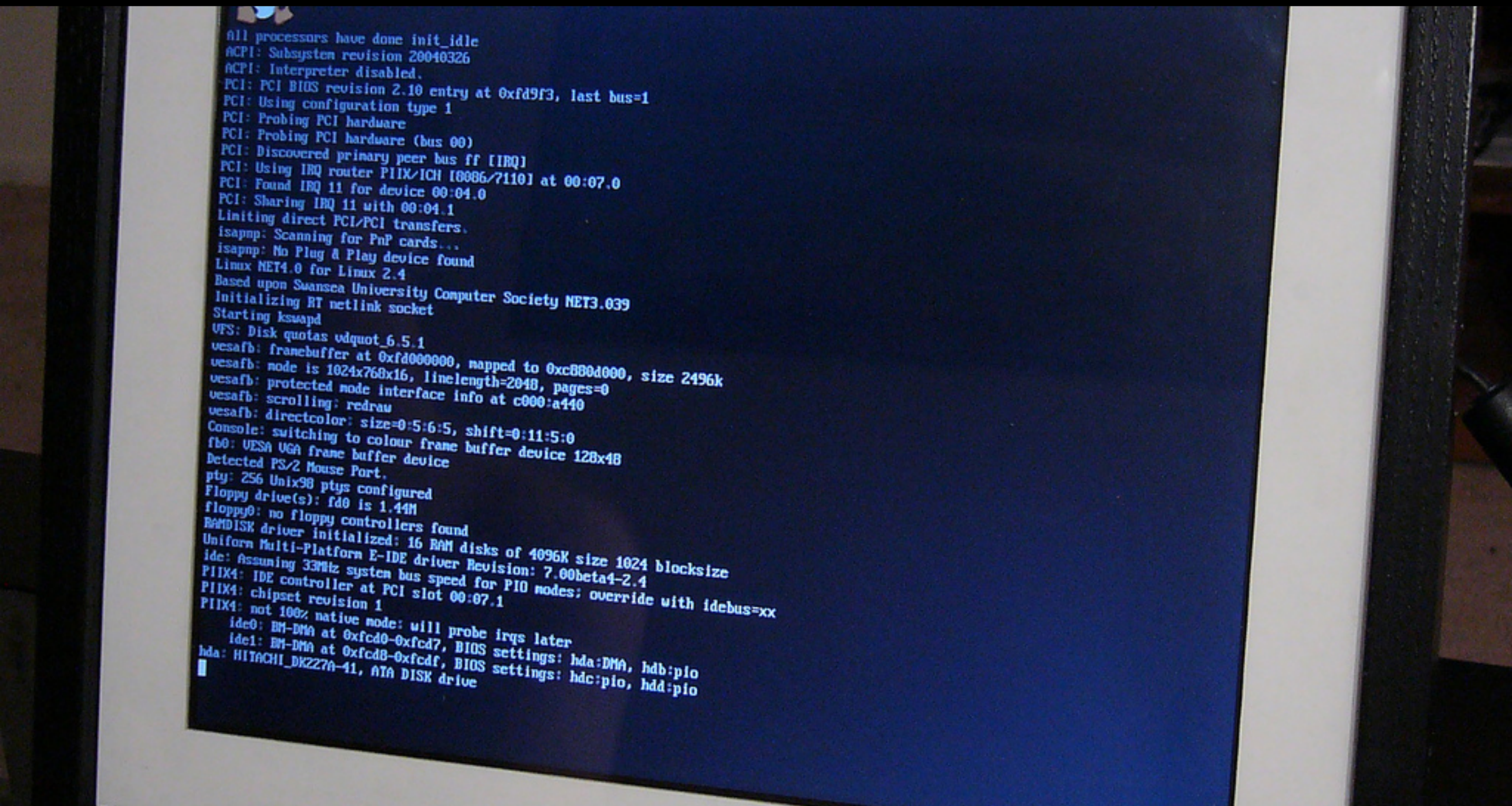
WHAT DO I MEAN?

- 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?

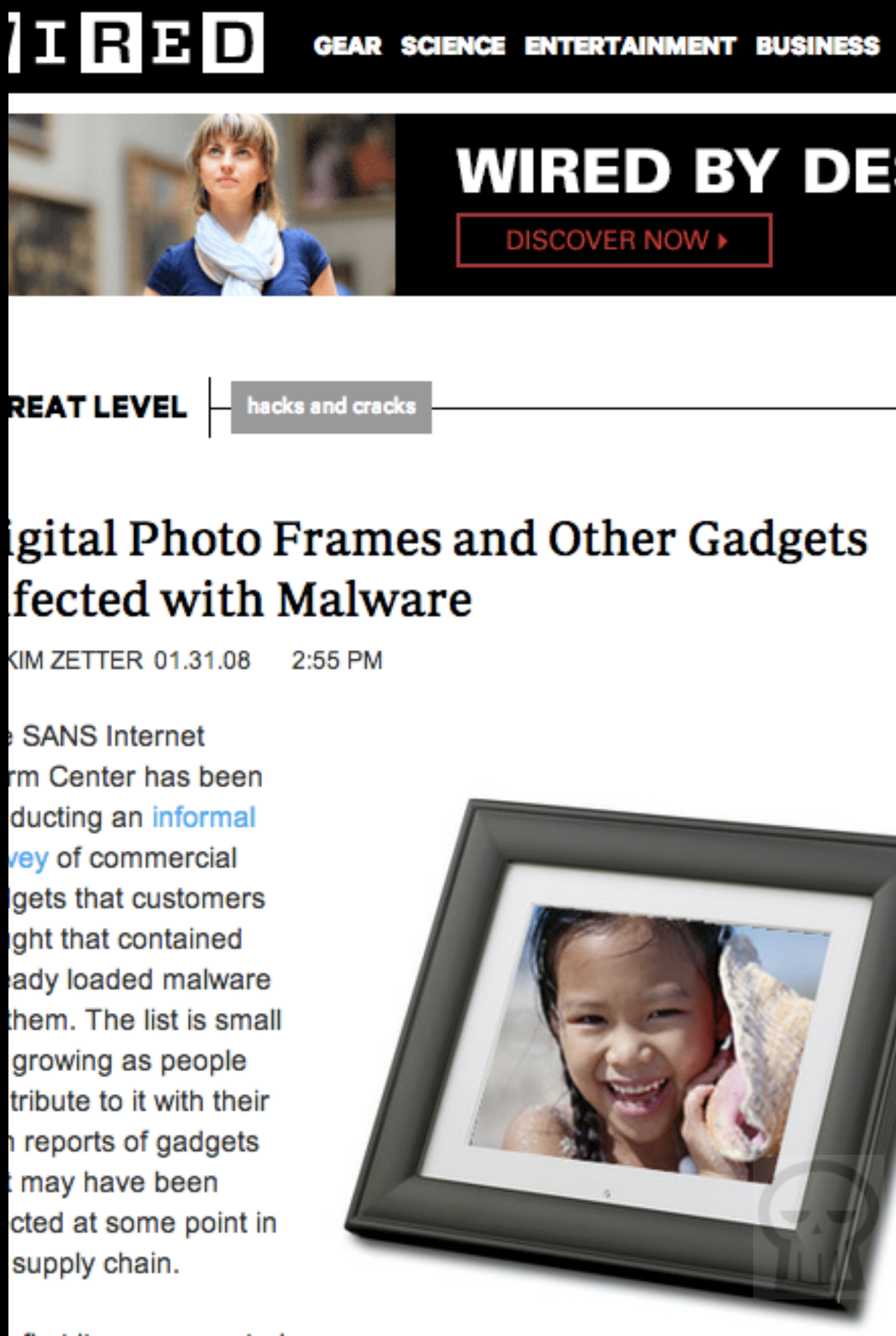
EXAMPLE OF A DIGITAL PICTURE FRAME OR USB DRIVE

HOW DID MY WIDGET GET HERE?



MALWARE IN THE PIPELINE...

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



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”

INTERNATIONAL STANDARD

ISO 28000

First edition
2007-09-15

Specification for security management systems for the supply chain

Spécifications pour les systèmes de management de la sûreté pour la chaîne d'approvisionnement

ISO 28000:2007

- ISO 28000:2007 specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain.

- Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security.

- These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

ISO 28000 HIGHLIGHTS

- Establish, implement, maintain and improve a security management system
- Assure conformance with stated security management policy
- Demonstrate such conformance to others
- Seek certification/registration of its security management system by an Accredited third party Certification Body; or
- Make a self-determination and self-declaration of conformance with ISO 28000:2007

OUR FLANK? WHAT FLANK?

THE MAGINOT LINE

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?

...OR THIS?

THINGS LIKE DOCKER WILL HELP... RIGHT?

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

WAR STORY

- External Penetration Test
- Partner connections to $MyDayJob were all tested.
- Testers were able to gain access to $MyDayJob network
- username: $vendor, password: <blank>

WHAT WENT WRONG

- Default configurations in place
- No verification of the security controls in place
- No active testing of partner connections
- No contractual language pertaining to third party connections

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.

I DON’T WANT TO POINT FINGERS BUT...

BLUE COAT & SYRIA

- "U.S. Firm Acknowledges Syria Uses Its Gear to Block Web" Wall Street Journal (http://online.wsj.com/news/articles/SB10001424052970203687504577001911398596328)

- "Update On Blue Coat Devices In Syria" Bluecoat (http://www.bluecoat.com/company/news/update-blue-coat-devices-syria)

- "Blue Coat Partner Fined $2.8m Over Syria Surveillance Sales" TechWeek EU (http://www.techweekeurope.co.uk/news/blue-coat-partner-fined-surveillance-syria-114548)

- Exposed by hacktivists. Admitted failure. Fines applied.

ATM, FAVORITE OF NE'ER DO WELLS

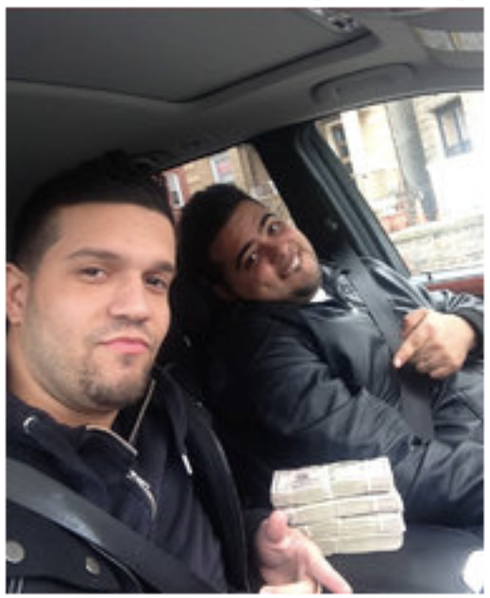
ANOTHER LEGAL ISSUE EXAMPLE, ATM FRAUD

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

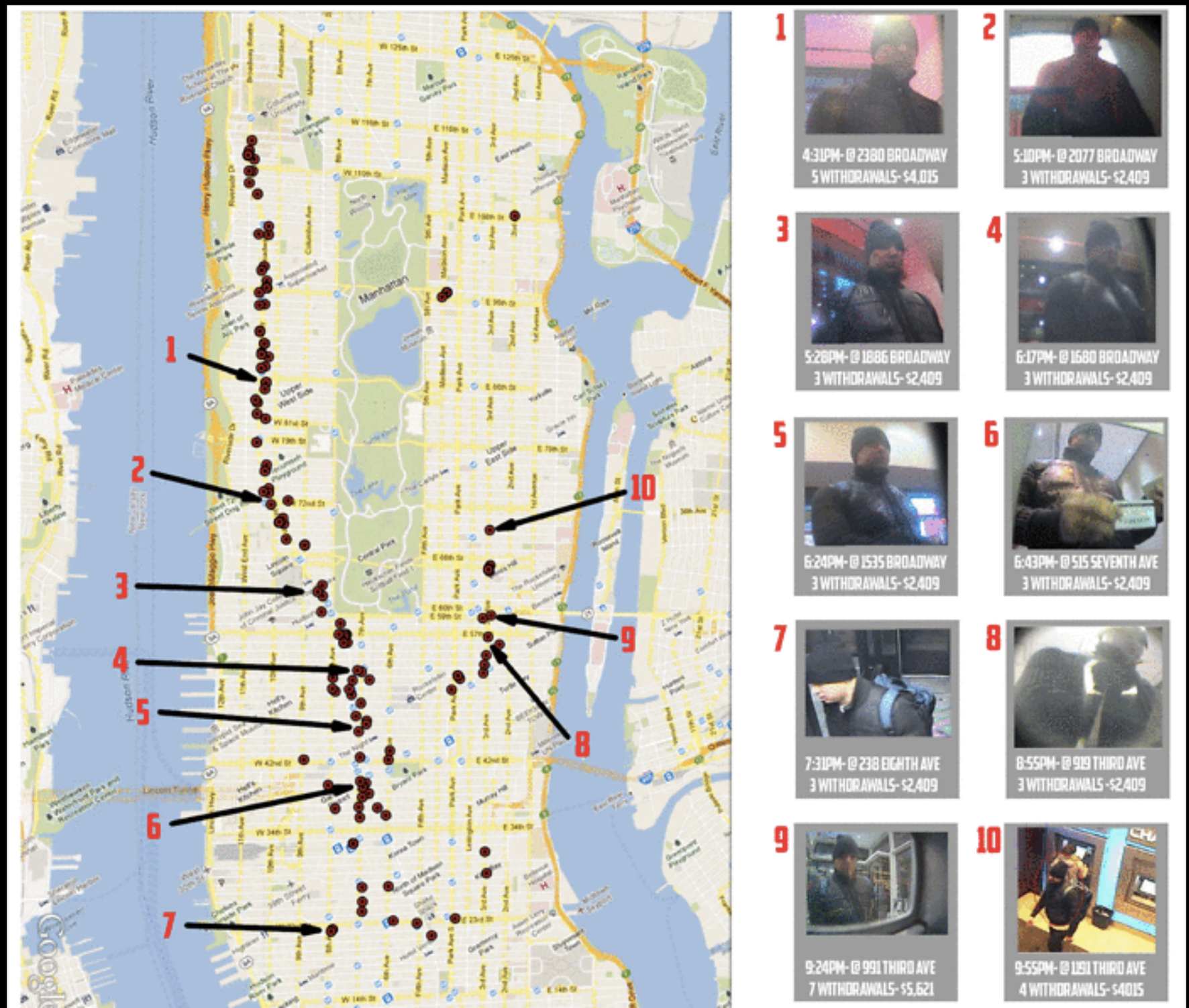
Elvis Rafael Rodriguez, left, and Emir Yasser Yeje, two of those charged in Brooklyn on Thursday, posed in March with approximately $40,000 in cash that the authorities say they were laundering.

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.

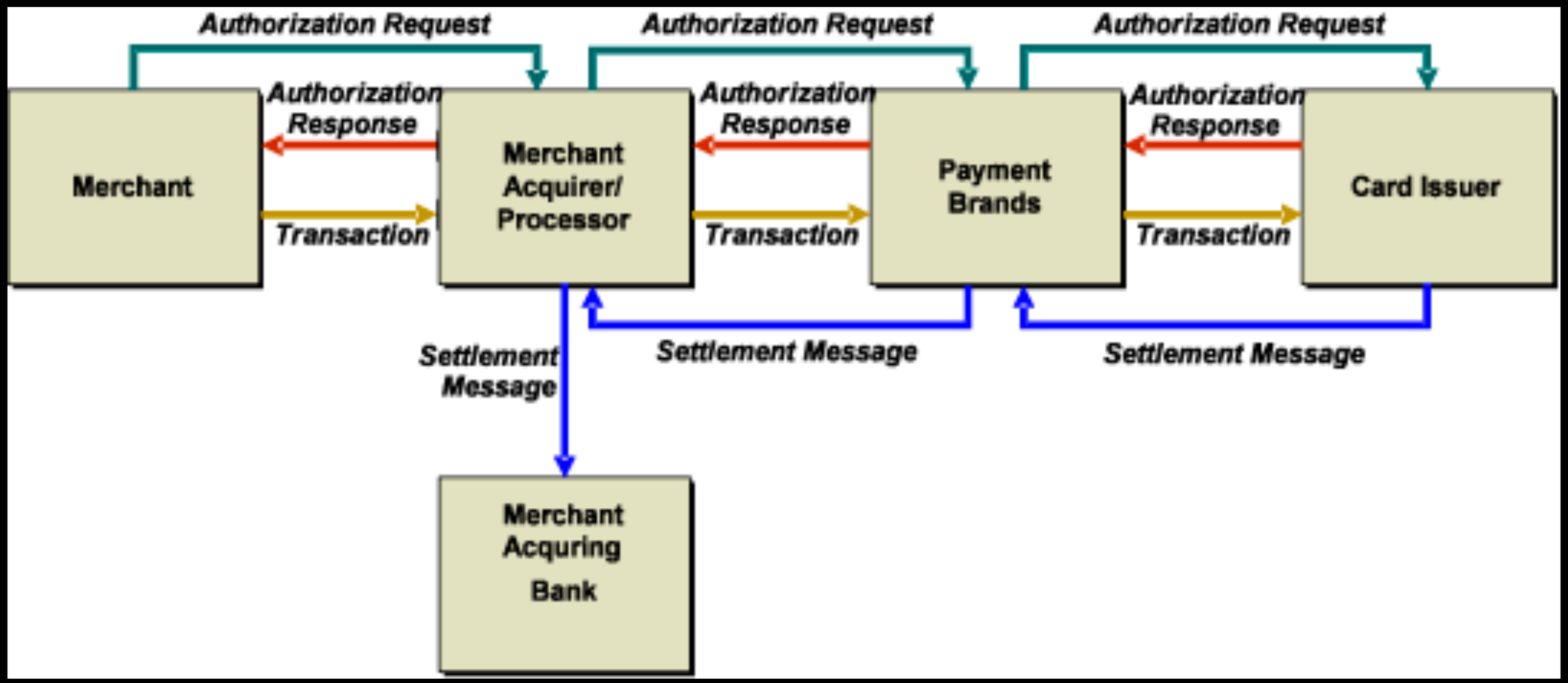
In New York City alone, the thieves responsible for A.T.M. withdrawals struck 2,904 machines over 10 hours starting on Feb. 19, withdrawing $2.4 million.

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.

IT WAS QUICK


1
2
3
4
5
6
7
8
9
10
Manhattan
1
4:31PM- @ 2380 BROADWAY
5 WITHDRAWALS- $4,015
2
5:10PM- @ 2077 BROADWAY
3 WITHDRAWALS- $2,409
3
5:26PM- @ 1886 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- @ 919 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
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

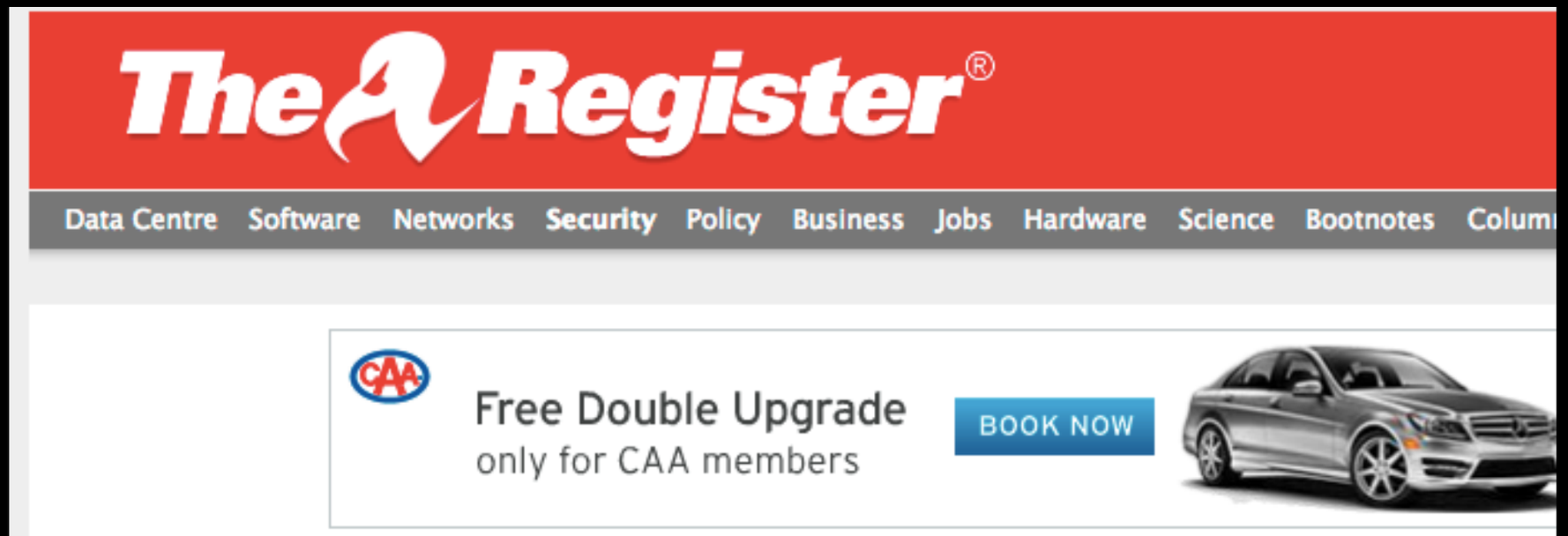
WHAT WENT WRONG?

- 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.

SNIPS IN THE WIRE



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.

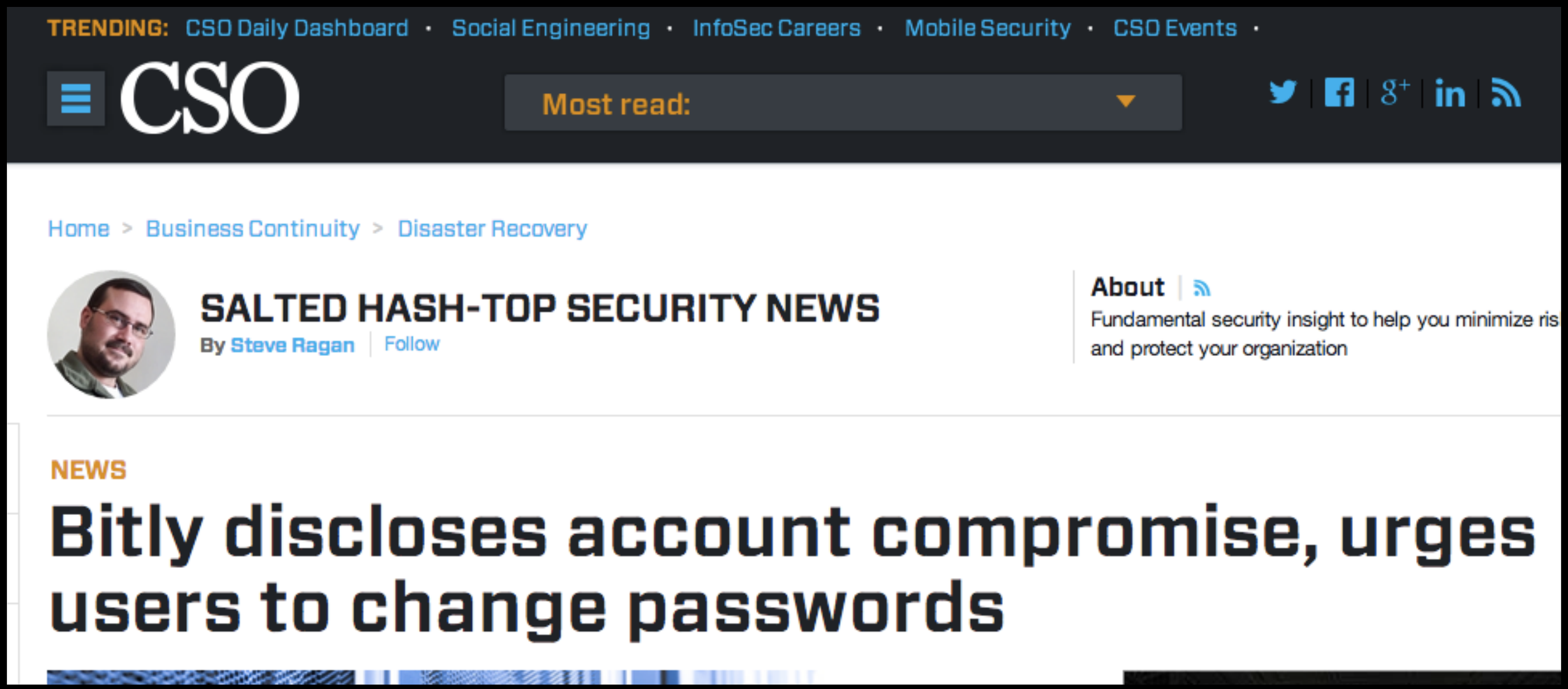
Affected Products

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

WAR STORY

- Magical Support Elves on outsourced software development contract
- Remote access via VPN and RSA tokens for authentication
- Faster than a speeding developer...

THE LOGINS

Chennai – 6:43 pm

Hyderabad – 6:52 pm

Mumbai – 7:09 pm

Goa – 7:22 pm

Pune – 7:41 pm

Bangalore – 7:55 pm

SPACE & TIME

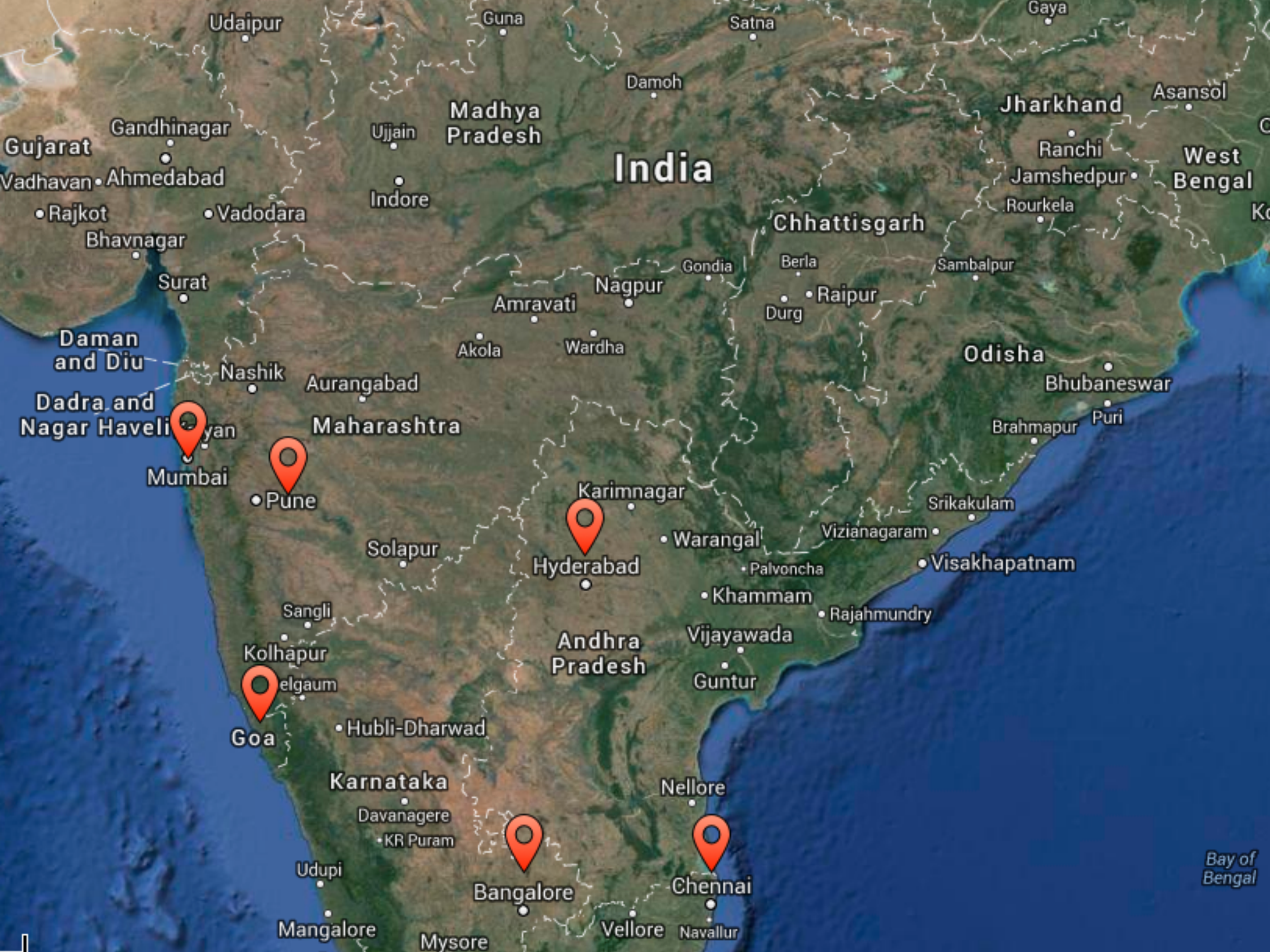
Chennai – Hyderabad = 633 km journey of 9 hours 36 min, in 9 min

Hyderabad – Mumbai = 708 km journey of 11 hrs 12 min, in 11 min

Mumbai – Goa = 604 km journey of 9 hrs and 28 min, in 13 min

Goa – Pune = 457 km journey of 7 hrs and 33 min, in 18 min

Pune – Bangalore = 836 km journey of 11 hrs and 20 min...in 14 minutes.


Udaipur
Guna
Satna
Gaya
Damoh
Asansol
Madhya Pradesh
Jharkhand
Gandhinagar
Gujarat
Ujjain
India
Ranchi
West Bengal
Vadhavan
Ahmedabad
Jamshedpur
Indore
Rajkot
Vadodara
Rourkela
Chhattisgarh
Bhavnagar
Berla
Gondia
Sambalpur
Surat
Nagpur
Raipur
Amravati
Durg
Daman and Diu
Akola
Wardha
Odisha
Nashik
Bhubaneswar
Aurangabad
Dadra and Nagar Haveli
Maharashtra
Puri
Brahmapur
Mumbai
Karimnagar
Srikakulam
Pune
Vizianagaram
Warangal
Solapur
Hyderabad
Visakhapatnam
Palvoncha
Khammam
Sangli
Rajahmundry
Andhra Pradesh
Vijayawada
Kolhapur
Guntur
Goa
Hubli-Dharwad
Karnataka
Nellore
Davanagere
KR Puram
Udupi
Bangalore
Chennai
Bay of Bengal
Mangalore
Vellore
Navallur
Mysore

THE CATCH

- What was the common theme between these contractors?

- They all used the **SAME** login

WHAT WENT WRONG

- Contractors were not clearly trained regarding security awareness
- Contractors shared the same login credentials
- Active monitoring was not in place
- The company did not see fit to penalize the contractor as it would have negatively affected renewal negotiations.

We weren’t tackling the basics well.

We Failed

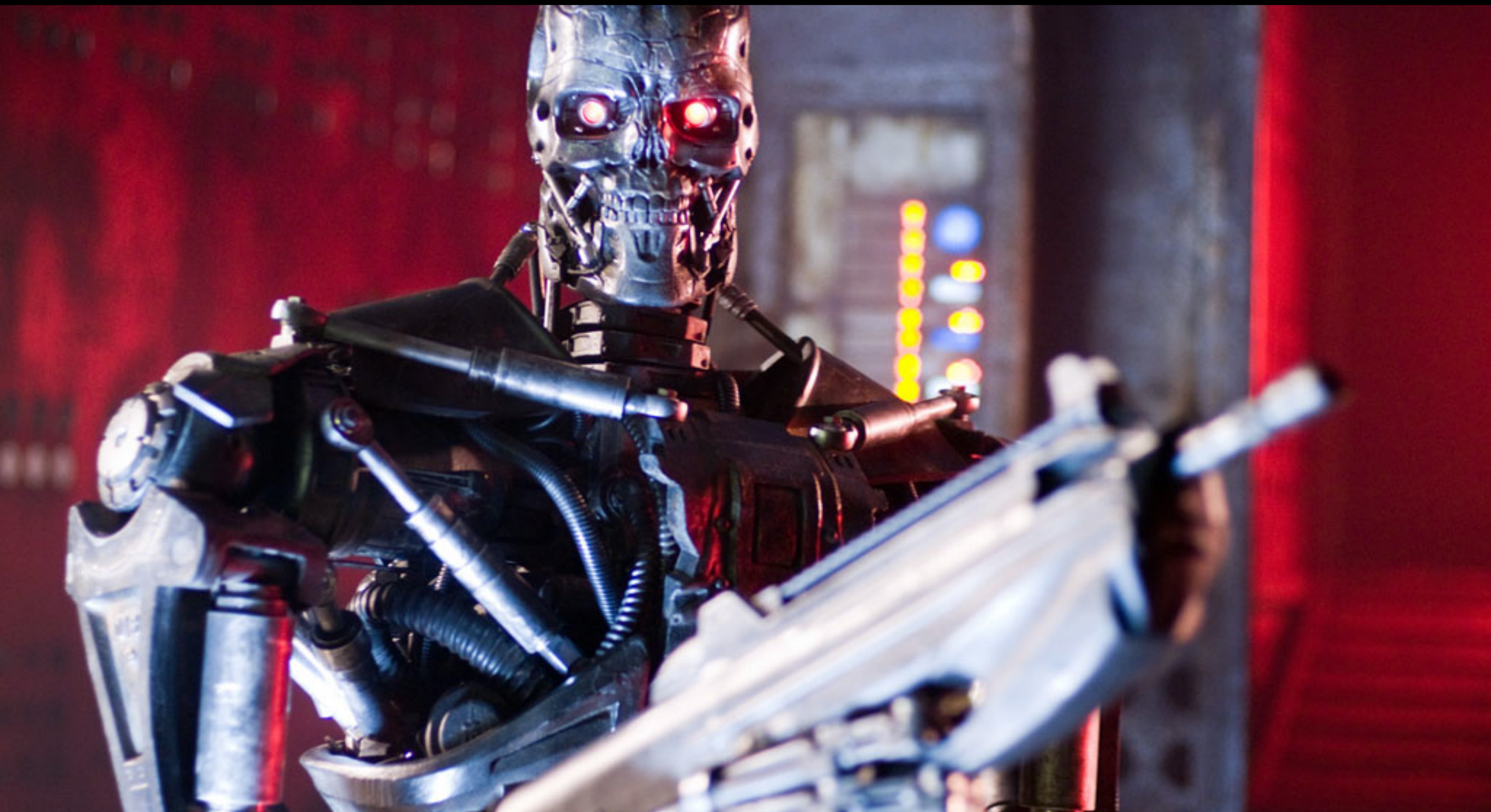
HARDWARE TROJANS

MORE RECENTLY...

BATTLEFIELD ROBOTS

OH...RIGHT

YIPES!



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

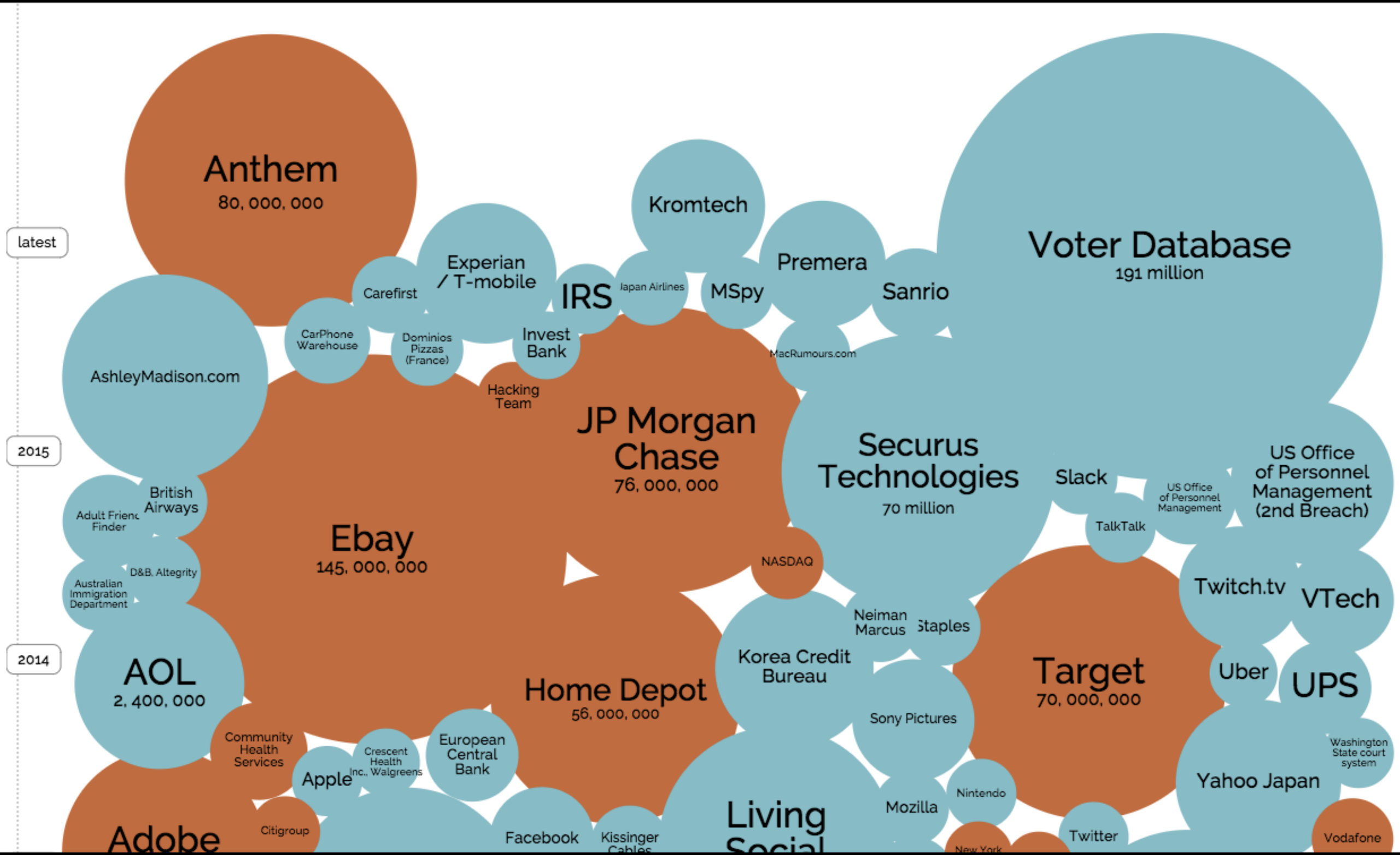
ISN'T THERE YET

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*

MORE RECENTLY

HOME DEPOT, TARGET, GOOD WILL


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

WHERE TO FROM HERE?

ACT III

GO BEYOND COMPLIANCE

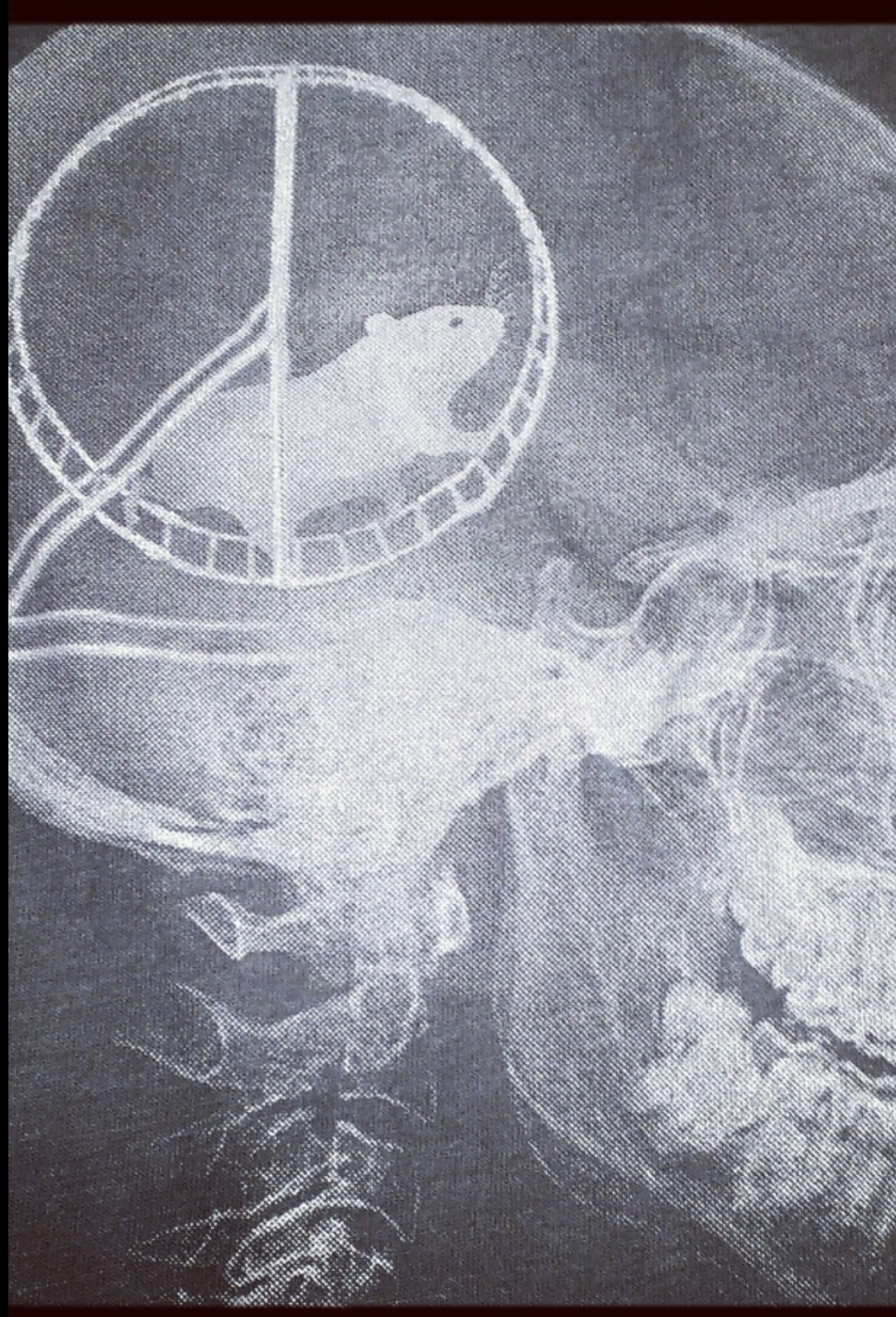
- Compliance regimes are to address the BARE MINIMUM

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?

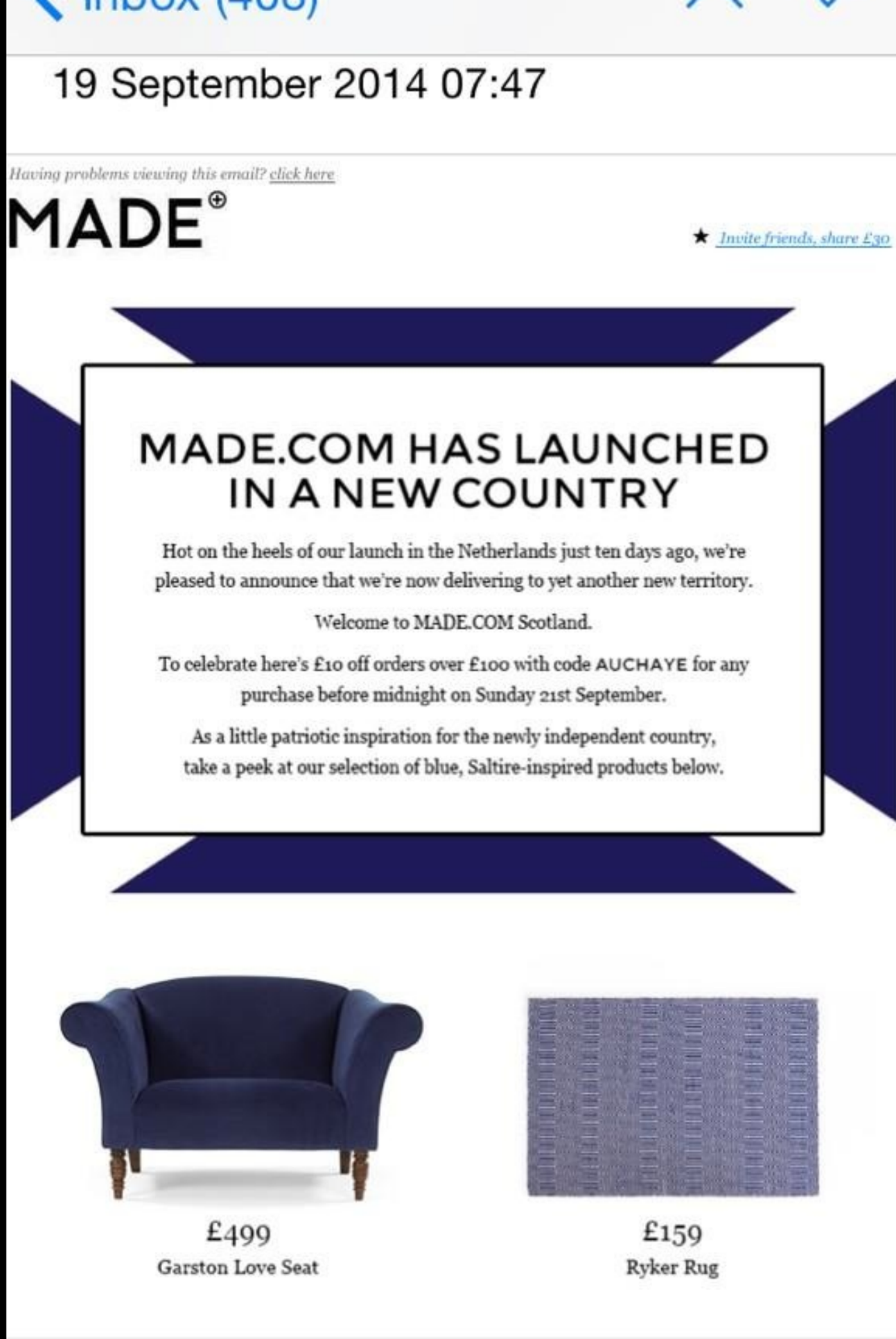
HAMSTER WHEEL OF PAIN

- 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
- At one org it was a perpetual game of keep away.
- 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 for listening

Thanks to BSides Ljubljana!

Questions?
Thanks

Dave Lewis
@gattaca

dave@akamai.com