

DEFENDING THE EXPOSED FLANK

DIGITAL SUPPLY CHAIN SECURITY

FIRST 2017



Hi

I'm Martin McKeay

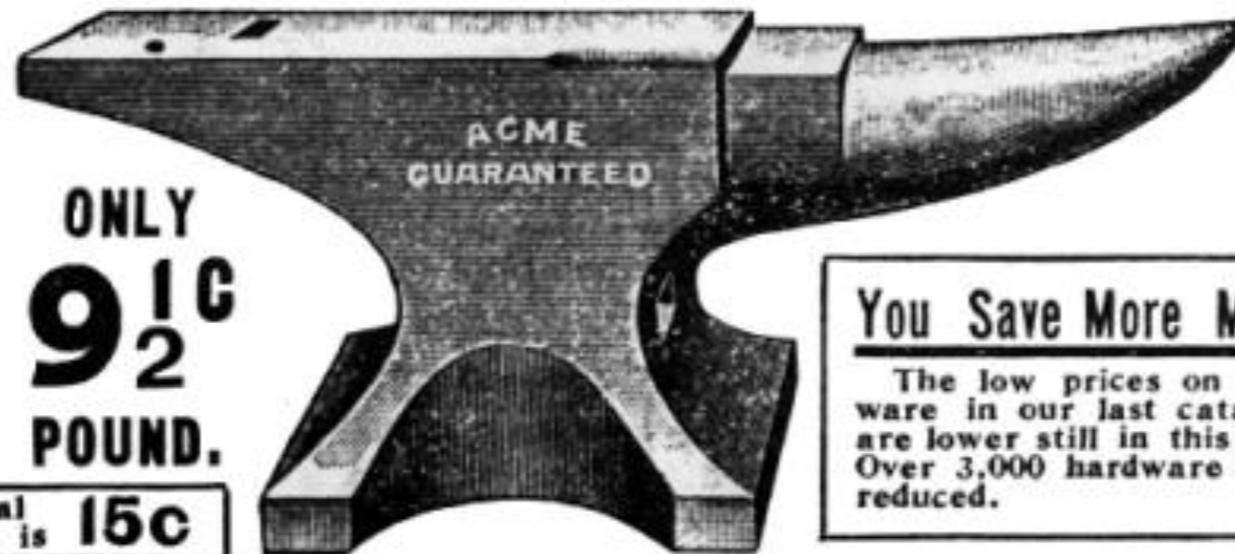
I have been in security for almost two decades

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
9¹/₂
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



HONNEST

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?

```
all processors have done init_idle
ACPI: Subsystem revision 20040326
ACPI: Interpreter disabled.
PCI: PCI BIOS revision 2.10 entry at 0xfd9f3, last bus=1
PCI: Using configuration type 1
PCI: Probing PCI hardware
PCI: Probing PCI hardware (bus 00)
PCI: Discovered primary peer bus ff [IRQ]
PCI: Using IRQ router PIIX/ICH [0006/7110] at 00:07.0
PCI: Found IRQ 11 for device 00:04.0
PCI: Sharing IRQ 11 with 00:04.1
Limiting direct PCI/PCI transfers.
isapnp: Scanning for PnP cards...
isapnp: No Plug & Play device found
Linux NET4.0 for Linux 2.4
Based upon Swansea University Computer Society NET3.039
Initializing RT netlink socket
Starting kswapd
UFS: Disk quotas wdquot_6.5.1
vesafb: framebuffer at 0xfd000000, mapped to 0xc880d000, size 2496k
vesafb: mode is 1024x768x16, linelength=2048, pages=0
vesafb: protected mode interface info at c000:a440
vesafb: scrolling: redraw
vesafb: directcolor: size=0:5:6:5, shift=0:11:5:0
Console: switching to colour frame buffer device 128x48
fb0: UESA UGA frame buffer device
Detected PS/2 Mouse Port.
pty: 256 Unix98 ptys configured
Floppy drive(s): fd0 is 1.44M
floppy0: no floppy controllers found
RAMDISK driver initialized: 16 RAM disks of 4096K size 1024 blocksize
Uniform Multi-Platform E-IDE driver Revision: 7.00beta4-2.4
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX4: IDE controller at PCI slot 00:07.1
PIIX4: chipset revision 1
PIIX4: not 100% native mode: will probe irqs later
   ide0: BM-DMA at 0xfc0-0xfc7, BIOS settings: hda:DMA, hdb:pio
   ide1: BM-DMA at 0xcd8-0xcdf, BIOS settings: hdc:pio, hdd:pio
hda: HITACHI_DK227A-41, ATA DISK drive
```

MALWARE IN THE PIPELINE...

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



WIRED BY DE

DISCOVER NOW ▶

GREAT LEVEL

hacks and cracks

Digital Photo Frames and Other Gadgets Infected with Malware

KIM ZETTER 01.31.08 2:55 PM

The SANS Internet Storm Center has been conducting an [informal survey](#) of commercial gadgets that customers might find that contained pre-installed malware. The list is small but growing as people contribute to it with their reports of gadgets that may have been infected at some point in the supply chain.



OR WORSE...

POOR SECURITY IN CODE

```
// Set up passwords
add_auth_entry("\x50\x40\x40\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x50\x40\x40\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
add_auth_entry("\x50\x40\x40\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\x40\x40\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
add_auth_entry("\x50\x40\x40\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5); // root xmhdipc
add_auth_entry("\x50\x40\x40\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5); // root default
add_auth_entry("\x50\x40\x40\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5); // root juantech
add_auth_entry("\x50\x40\x40\x56", "\x13\x10\x11\x16\x17\x14", 5); // root 123456
add_auth_entry("\x50\x40\x40\x56", "\x17\x16\x11\x10\x13", 5); // root 54321
add_auth_entry("\x51\x57\x52\x52\x40\x50\x56", "\x51\x57\x52\x52\x40\x50\x56", 5); // support support
add_auth_entry("\x50\x40\x40\x56", "", 4); // root (none)
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x40\x50\x46", 4); // admin password
add_auth_entry("\x50\x40\x40\x56", "\x50\x40\x40\x56", 4); // root root
add_auth_entry("\x50\x40\x40\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\x40\x40\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 and more products delivered to us faster and cheaper the scale of operations has gone to 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.

[FACEBOOK](#)

[TWITTER](#)

[GOOGLE+](#)

[SAVE](#)

[EMAIL](#)

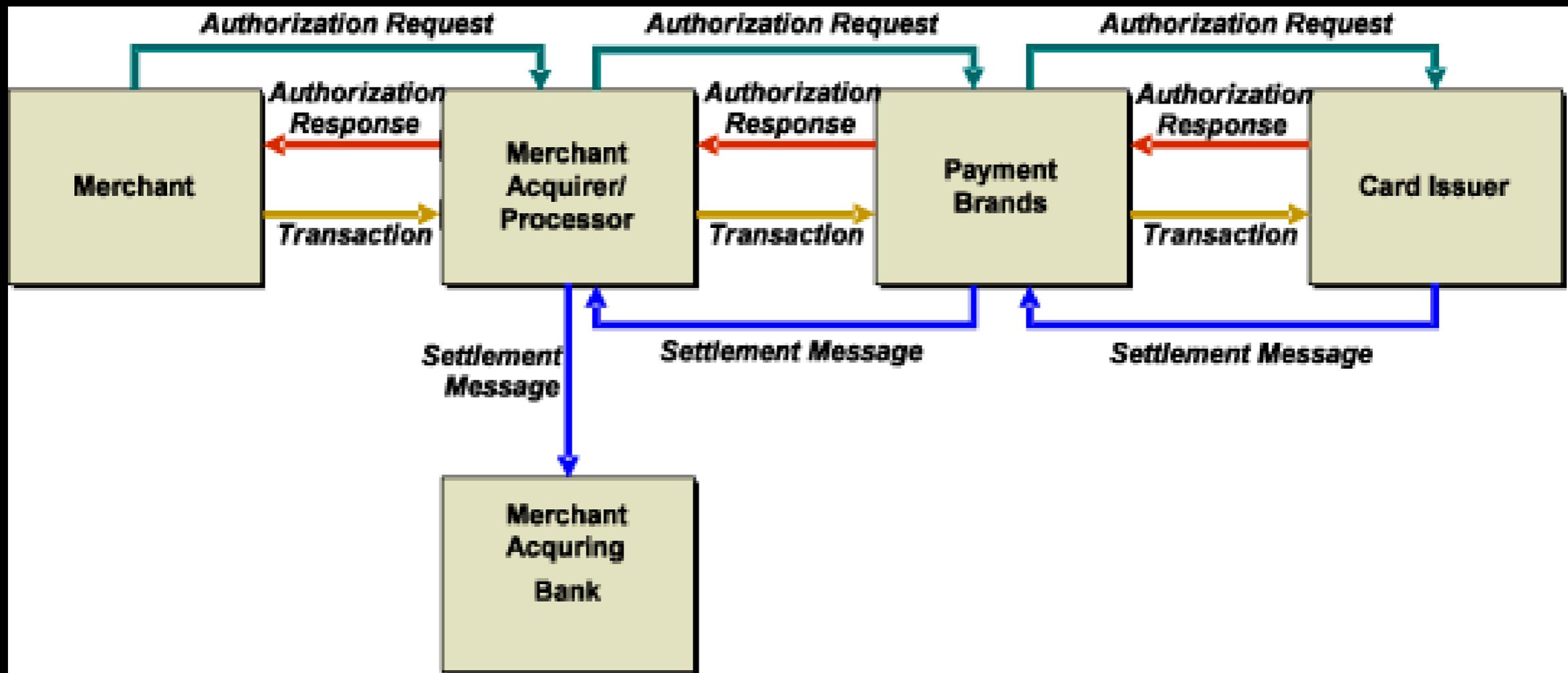
[SHARE](#)

[PRINT](#)

[REPRINTS](#)

BELLE
GET TICKETS

THE FLOW



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
---------	---------

Security Response Blog

Stay on top of Internet security trends

[Learn More >](#)

The Symantec Intelligence Report

Monthly report concerning malware, spam and other threats.

[More info >](#)

...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 risk 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

White Papers Webcasts Newsletters Resea

COMPUTERWORLD

Topics ▾ News In Depth Reviews Blogs ▾ Opinion Share

Hardware Computer Peripherals Laptops Macintosh Netbooks PCs Processors

SALARY SURVEY 2014 What's your earning power? Take

Home > Hardware > Processors

News

Security researchers create undetectable hardware trojans

Method can be used to weaken hardware random number generators used for encryption

By Jaikumar Vijayan

September 17, 2013 04:15 PM ET 7 Comments

[in](#) Share 17 [t](#) [g+1](#) [v](#) [d](#) [f](#) Like 110 [e](#) [More](#)

Computerworld - A team of security researchers from the U.S. and Europe has released a paper showing how integrated circuits used in computers, military equipment and other critical systems can be maliciously compromised during the manufacturing process through virtually undetectable changes at the transistor level.

As proof of the effectiveness of the approach, the paper describes how the

MORE RECENTLY...



BATTLEFIELD ROBOTS

White Papers | Webcasts | Newsletters | Research

COMPUTERWORLD

Topics ▾ | News | In Depth | Reviews | Blogs ▾ | Opinion | Shark

Applications | App Development | Big Data | Business Intelligence/Analytics | Content/Docu
Emerging Technologies | Enterprise Architecture | ERP | Open Source | Reg
Unified Communications

SALARY SURVEY 2014 | [Join our IT Salary Survey today and enter a drawing for 1 of 3 American Express gift cards](#)

Home > Applications > Emerging Technologies

News

U.S. military may have 10 robots per soldier by 2023

Military expects to soon be using autonomous robots to carry soldiers' gear and scan for enemy combatants

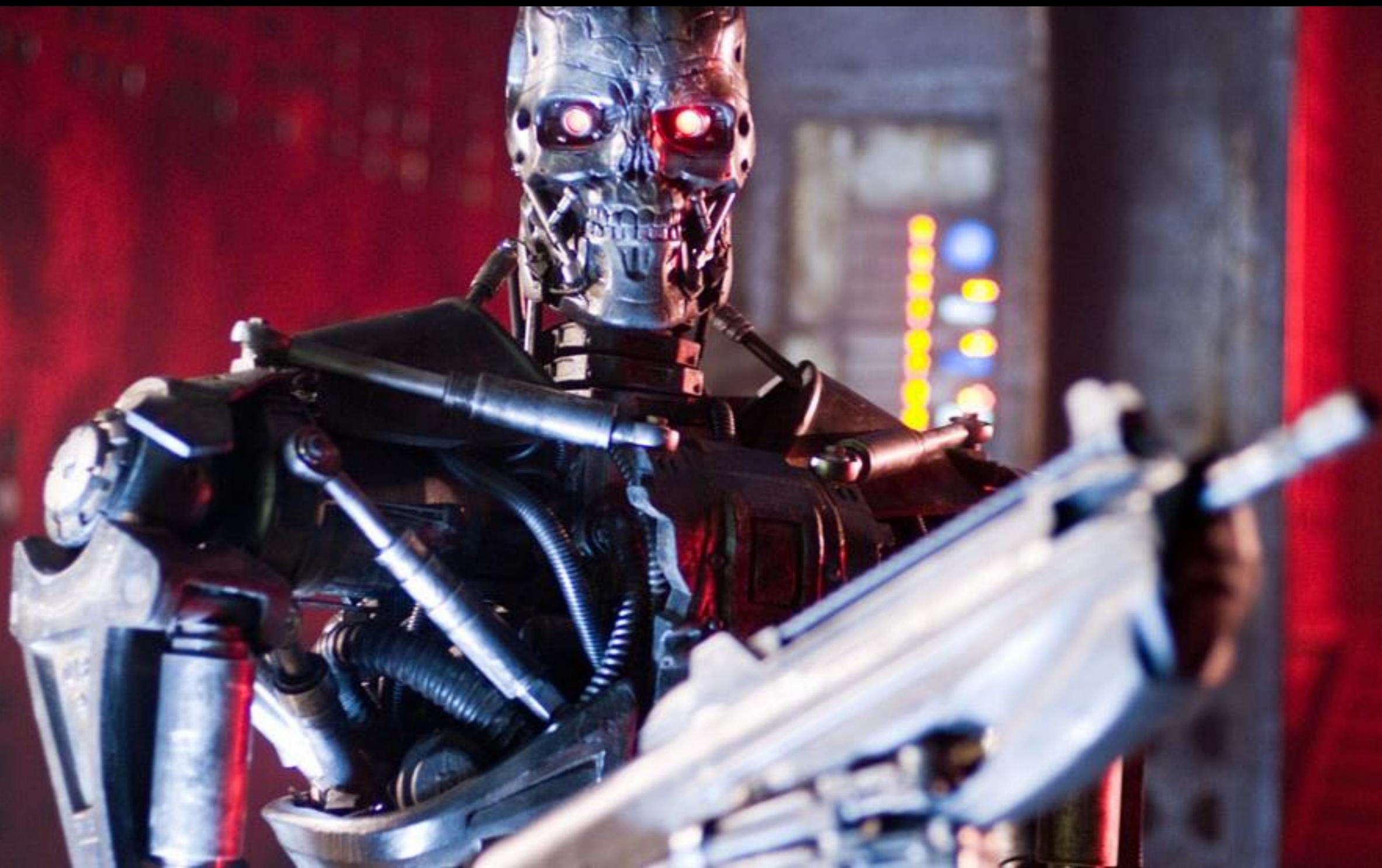
By Sharon Gaudin
November 14, 2013 05:32 PM ET | 4 Comments

[in](#) Share 12 | [t](#) | [g+1](#) | [v](#) | [d](#) | [f](#) Like 150 | [e](#) | [More](#)

Computerworld - American soldiers patrolling dangerous streets will soon be accompanied by [autonomous robots](#) programmed to scan the area with thermal imaging and send live images back to the command center.

Likewise, squads of infantrymen hiking through mountains will be helped by

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

[Share](#)

[Tweet](#)

[Email](#)

149



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

TWEET

SHARE (1,386)

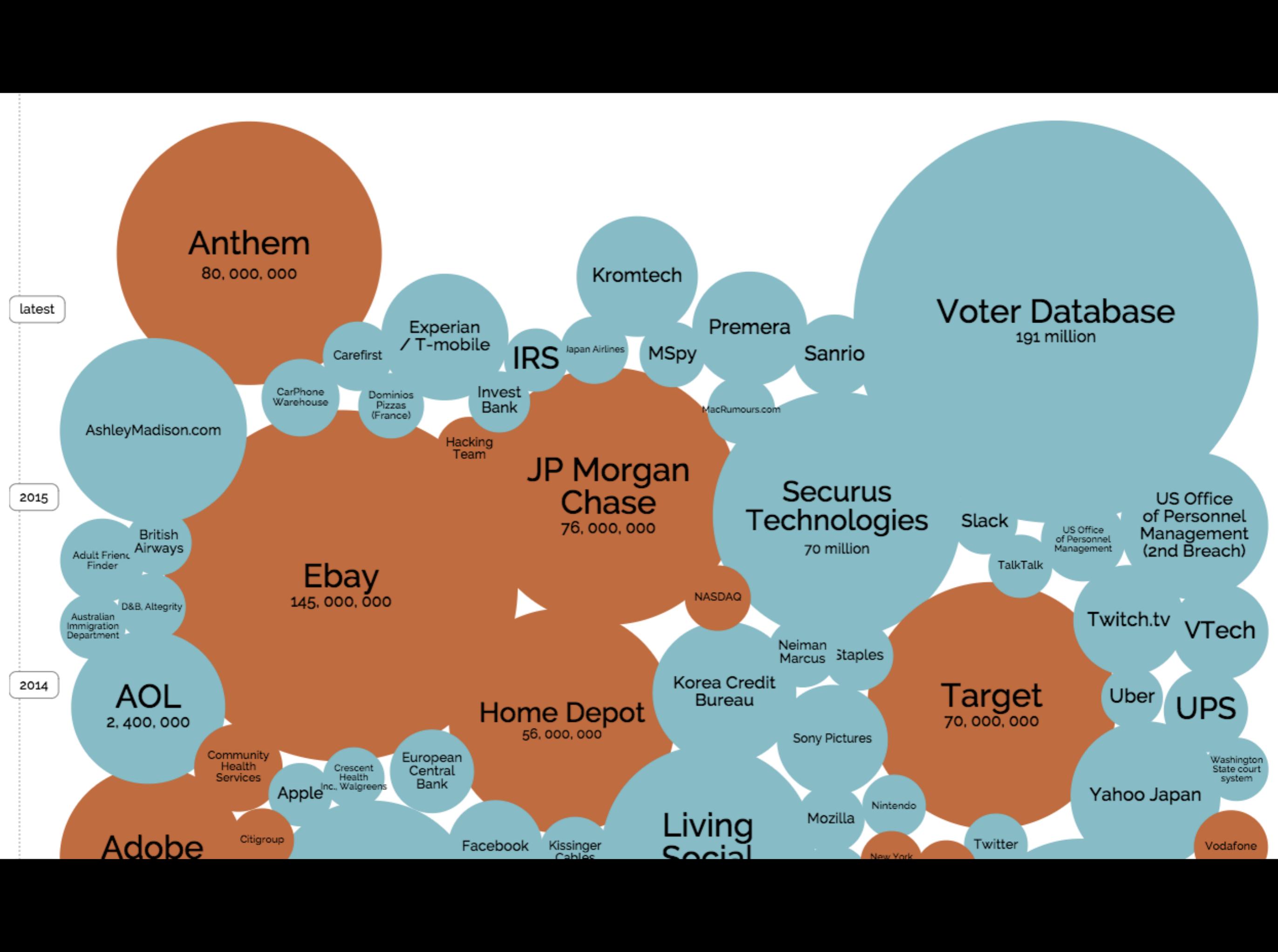
+



Most Viewed



4 states are voting today



WHERE TO FROM HERE?

ACT III



GO BEYOND COMPLIANCE

- Compliance regimes are to address the BARE MINIMUM

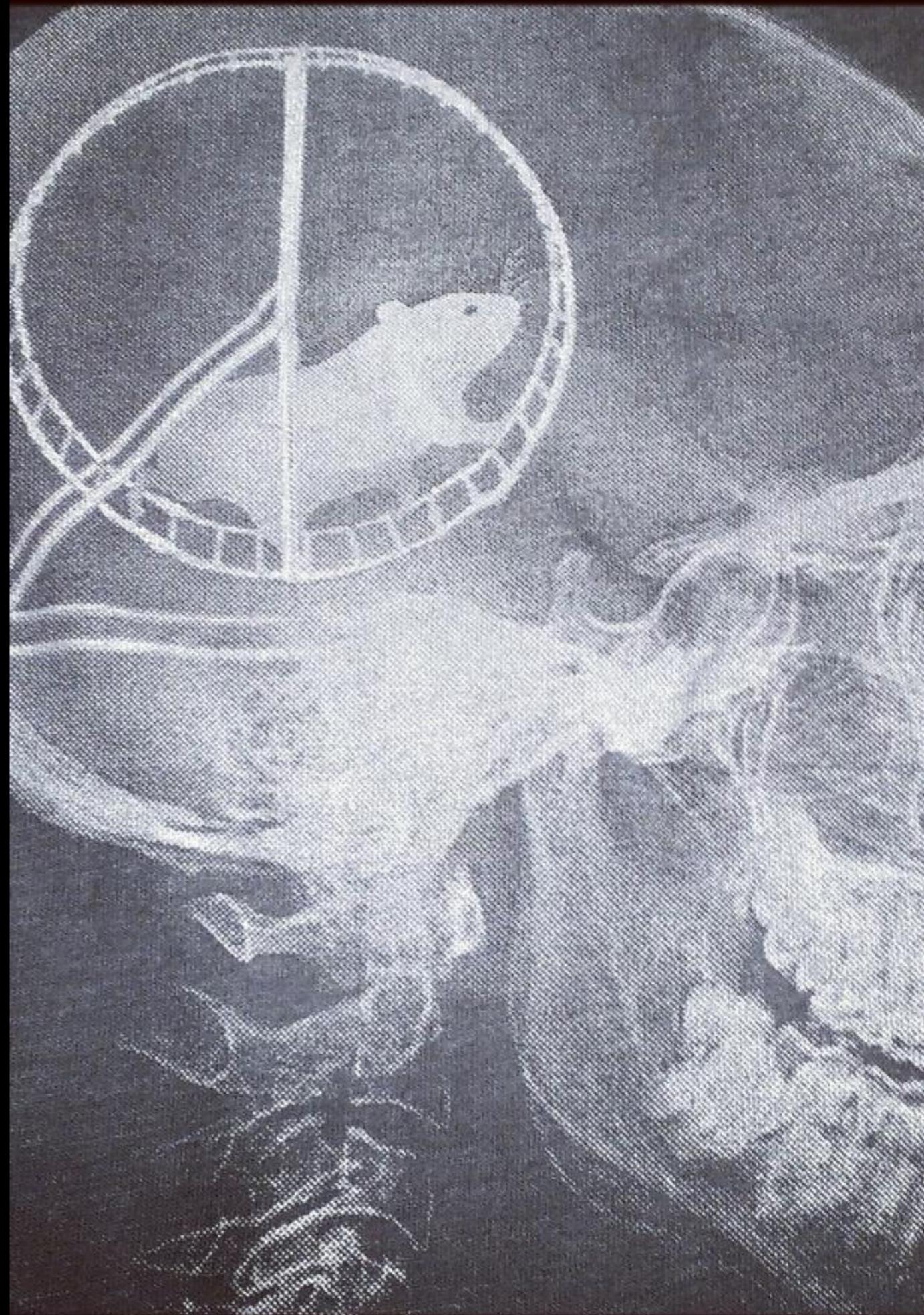


OFF SHORE DEVELOPMENT

- 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



19 September 2014 07:47

[Having problems viewing this email? click here](#)

MADE⁺

★ [Invite friends, share £30](#)

MADE.COM HAS LAUNCHED IN A NEW COUNTRY

Hot on the heels of our launch in the Netherlands just ten days ago, we're pleased to announce that we're now delivering to yet another new territory.

Welcome to MADE.COM Scotland.

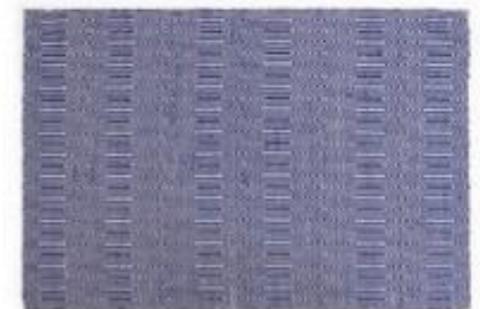
To celebrate here's £10 off orders over £100 with code **AUCHAYE** for any purchase before midnight on Sunday 21st September.

As a little patriotic inspiration for the newly independent country, take a peek at our selection of blue, Saltire-inspired products below.



£499

Garston Love Seat



£159

Ryker Rug

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.



SUCCESS

It can lead to fail

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!





Akamai

FASTER FORWARD

Questions?

Thanks

Martin McKeay

@mckeay

mmckeay@akamai.com