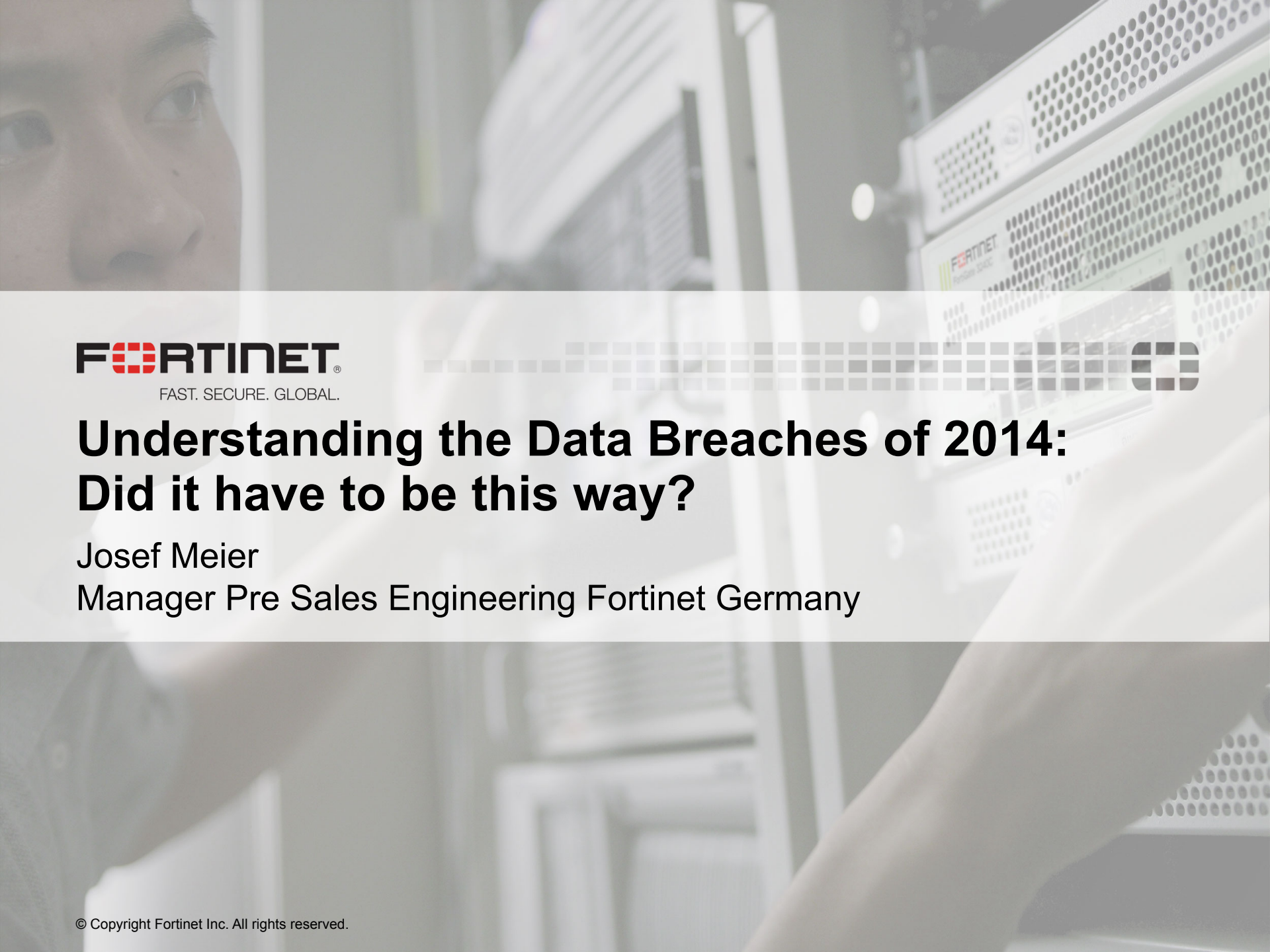


FAST. SECURE. GLOBAL.

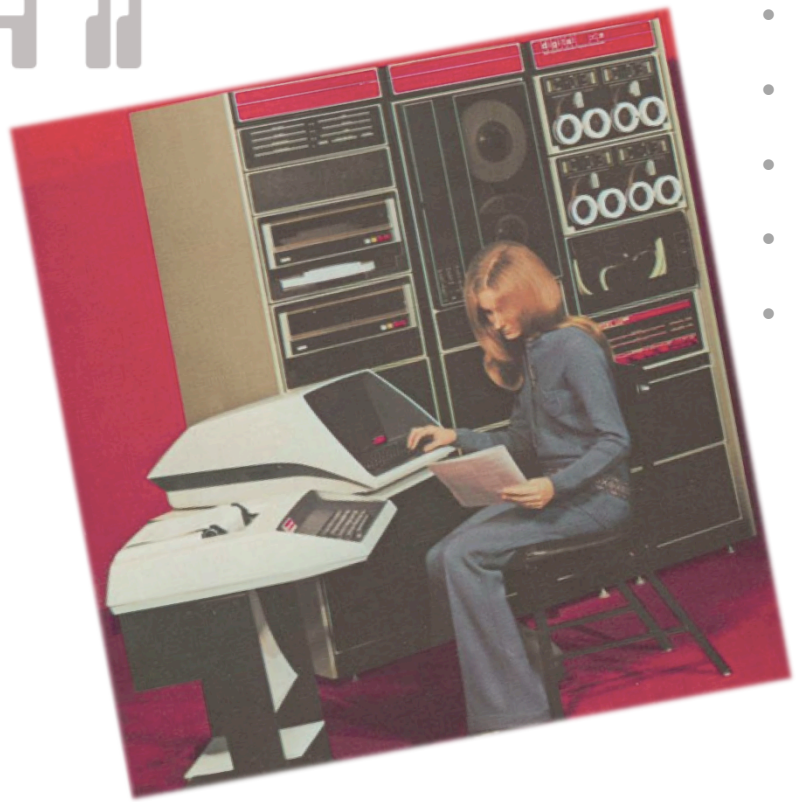
Understanding the Data Breaches of 2014: Did it have to be this way?

Josef Meier
Manager Pre Sales Engineering Fortinet Germany

The year?

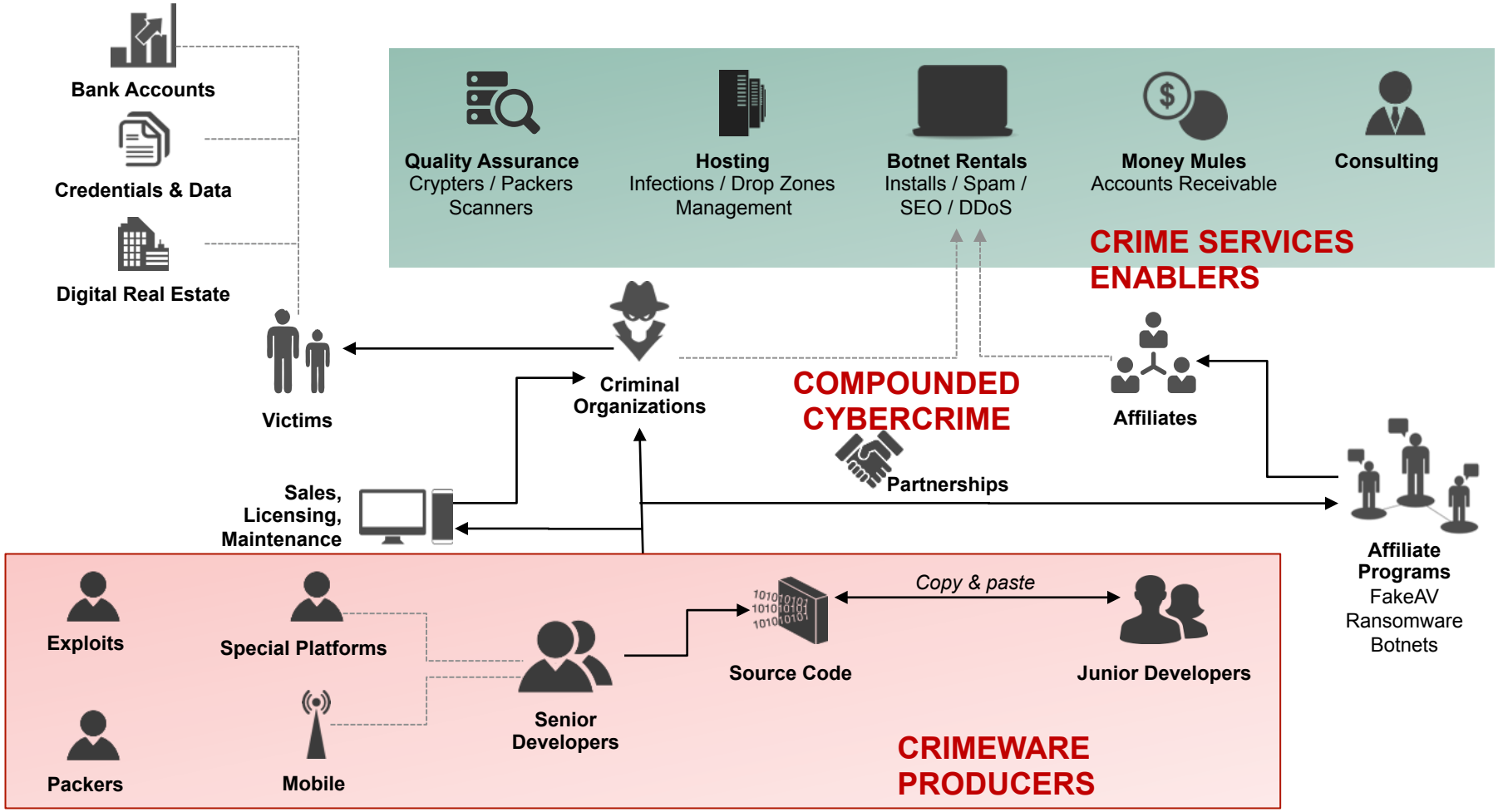
The Creeper – “Catch me if you can”…

1971

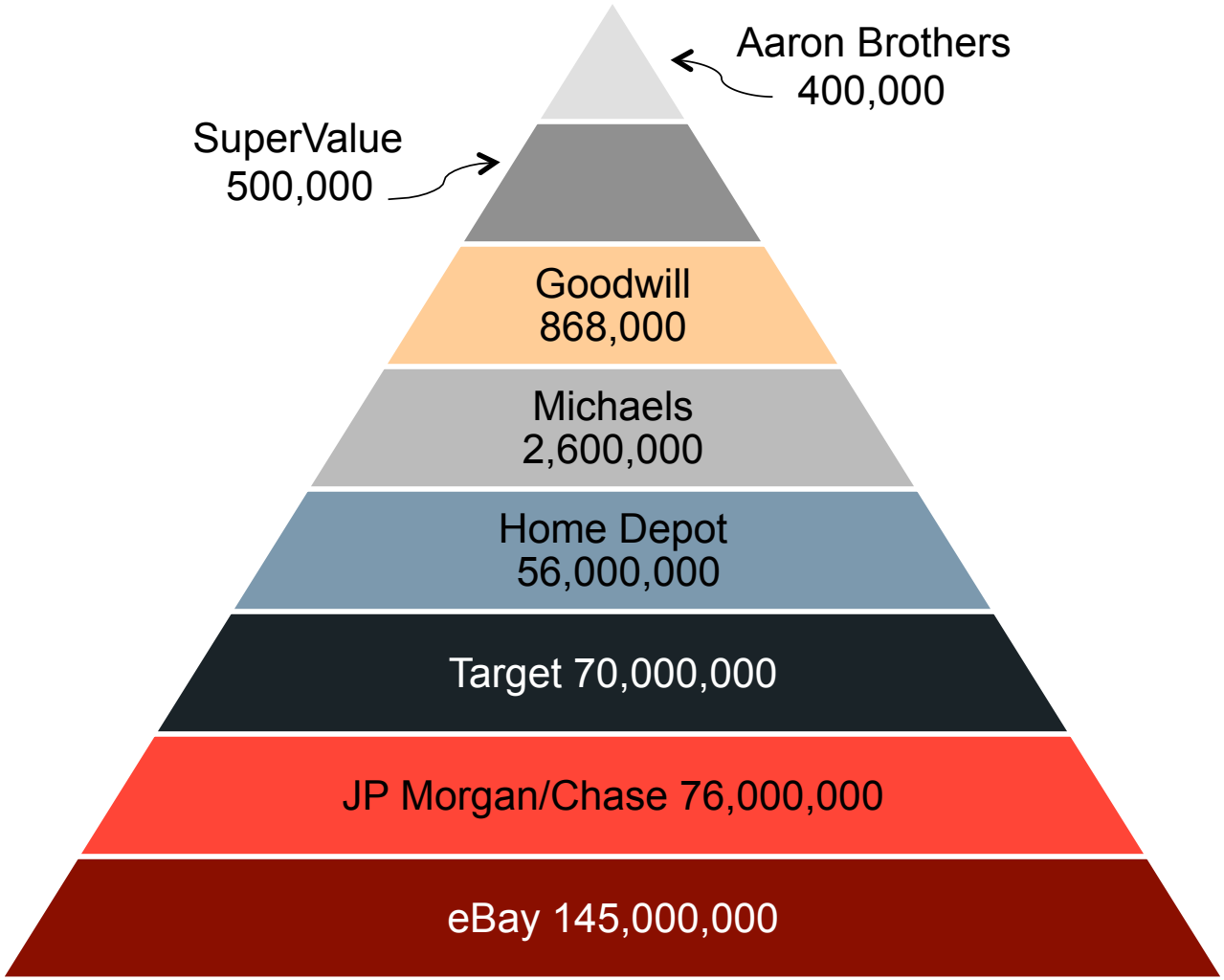


- Experimental self-replicating program
- Written in 1971 by Bob Thomas of BBN
- Infected DEC PDP-10 computers
- Just one year after unix epoch began
- ‘Reaper’ worm created in 1972 to delete it

Crimeware and Crime Services



Anyone Want To Add Anything?



*Milton Security

Point of Sale

- 2013 was the “year of the megabreach”
- Target and Home Depot made the headlines
- Between them details of 90 million credit cards stolen
- POS attacks still very prevalent

  small targets, large scale
- PCI 3.0 released in 2013 to reinforce protection

Finding the Common Thread

Target -
Outside contractor clicks on phishing email

http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p2

http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

Home Depot
Stolen login credentials from Third party vendor

http://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addreses/

http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html

JP Morgan/Chase –
Stolen employee credentials

http://www.computerworld.com/article/2862578/twofactor-authentication-oversight-led-to-jpmorgan-breach-investigators-reportedly-found.html

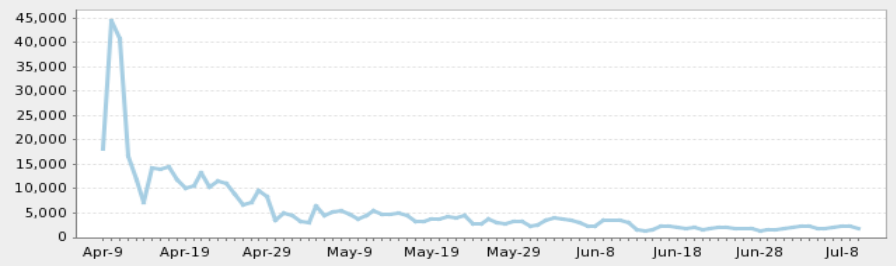
Industrial Malware

- Havex – the sequel to Stuxnet
- RAT (remote administration tool)
- Harvests information on hardware control systems (SCADA)

- OPC – OLE for Process Control
- Communication between Windows and control hardware
- OPC servers control machines via PLC

Server-side Attacks

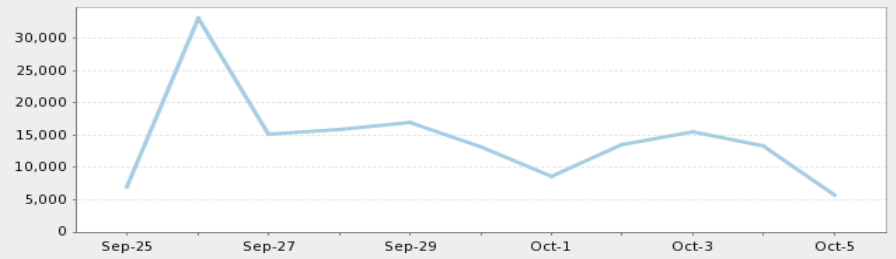
HeartBleed



500,000 Web Servers Affected

Time to Protect Critical
Surge in attacks while fresh

ShellShock

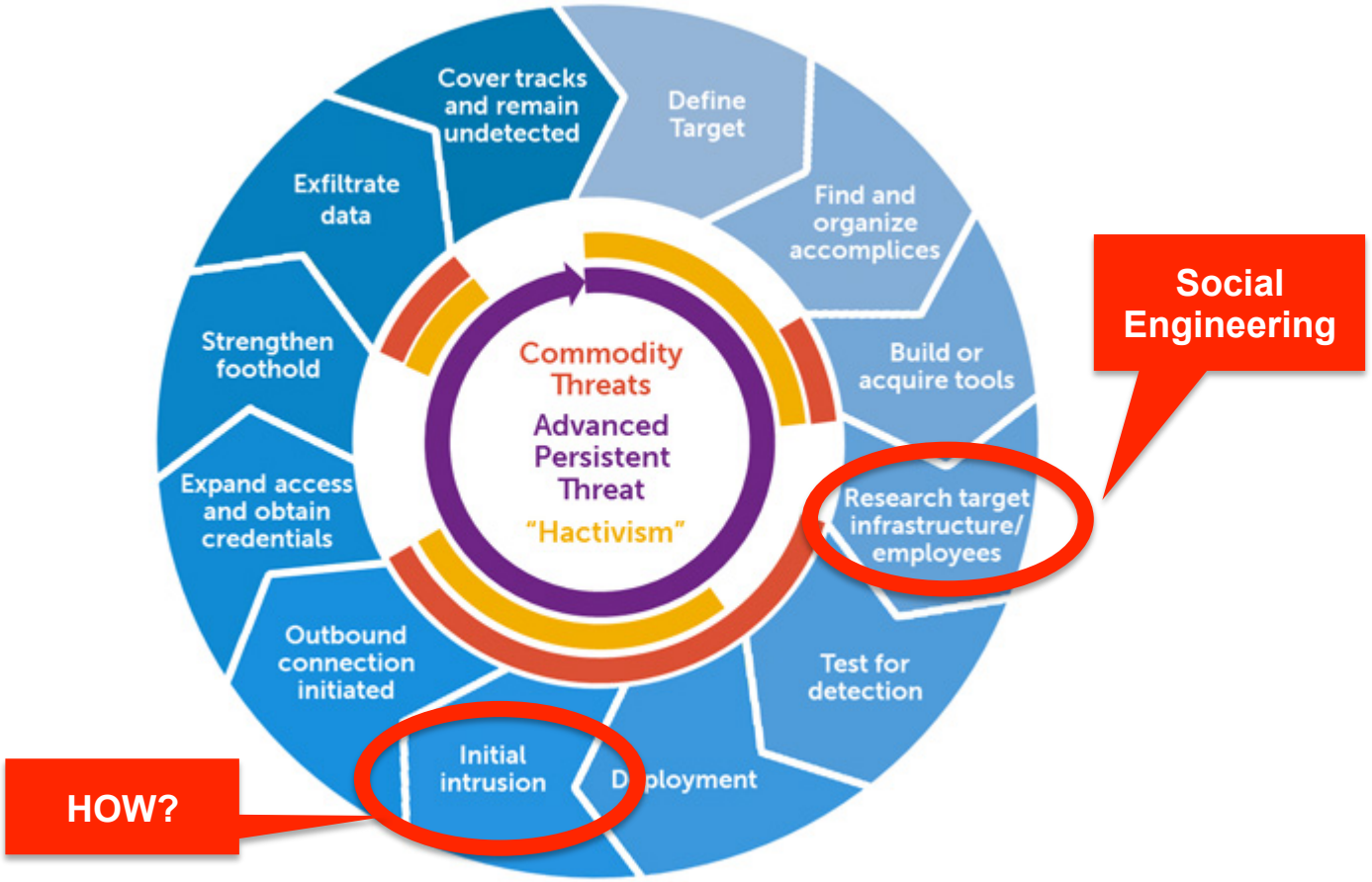


Millions of Internet Connected Devices Affected

Shellshock

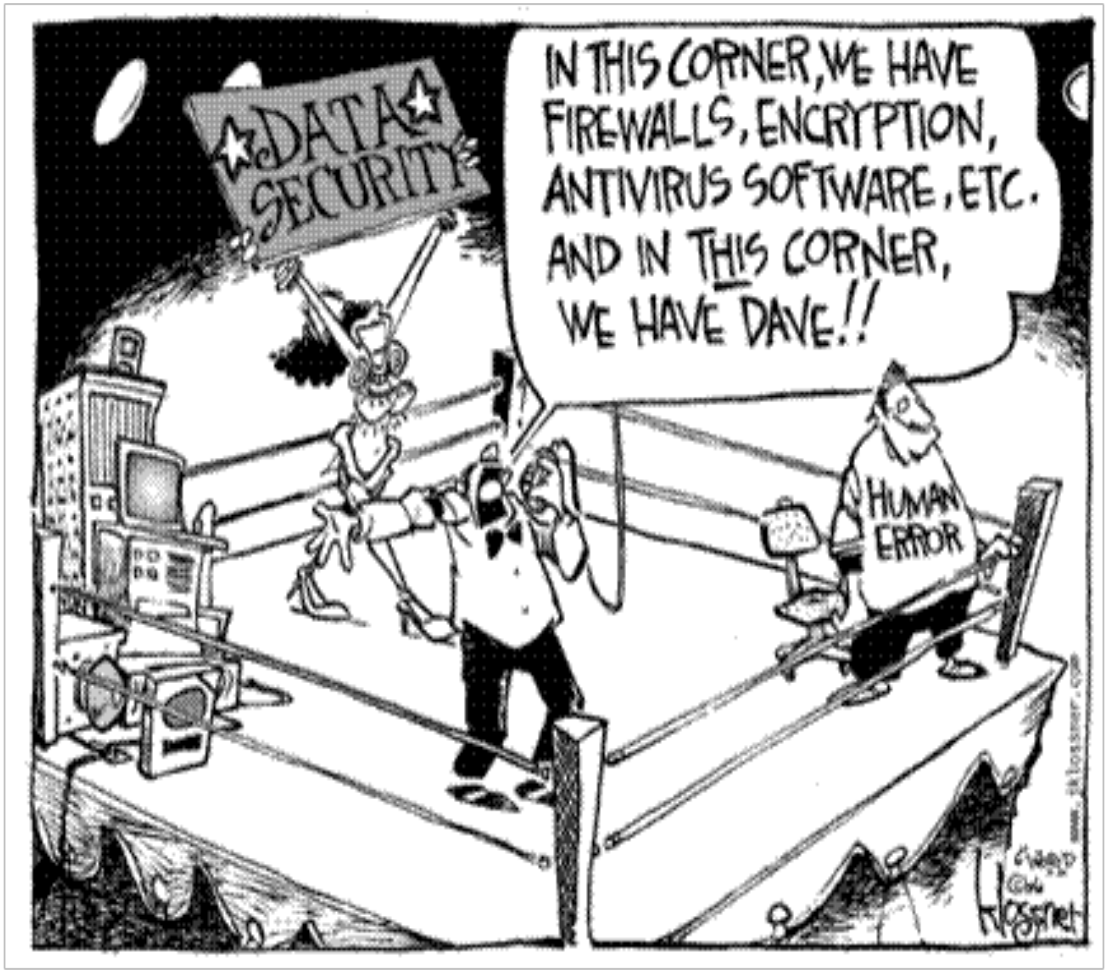
Devices

Advanced Persistent Threat Structure



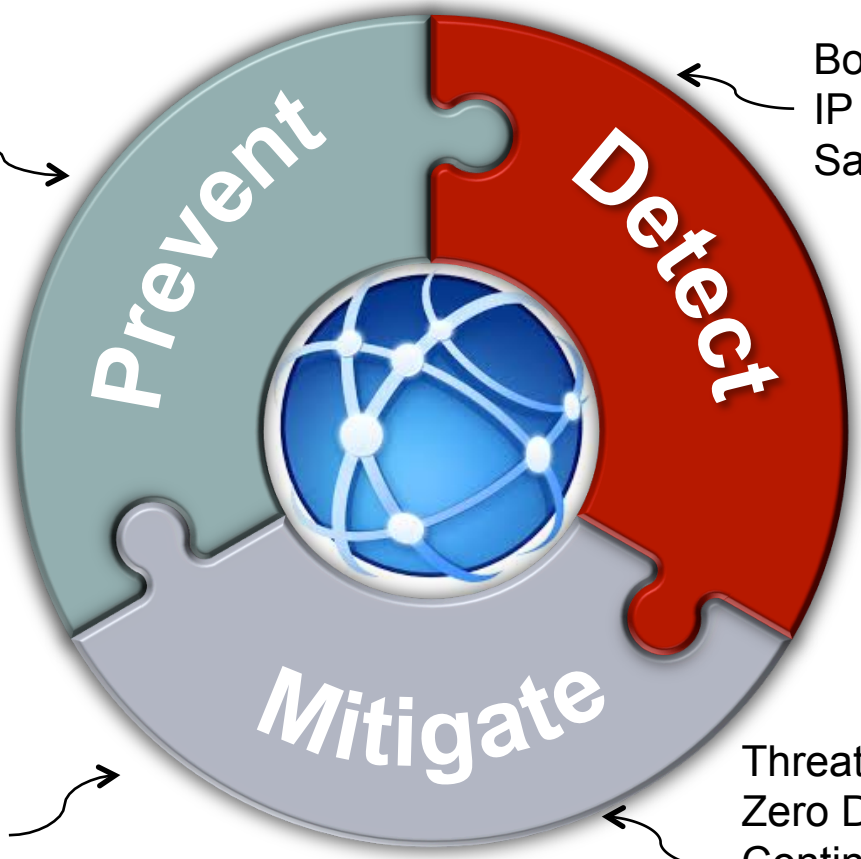
*Wikipedia Commons

Exploiting the Weak Link



The Technology Side of Things

Two Factor Authentication
Anti-Virus
Intrusion Prevention
Secure Email Gateway
Web Application Firewall
End Point Protection

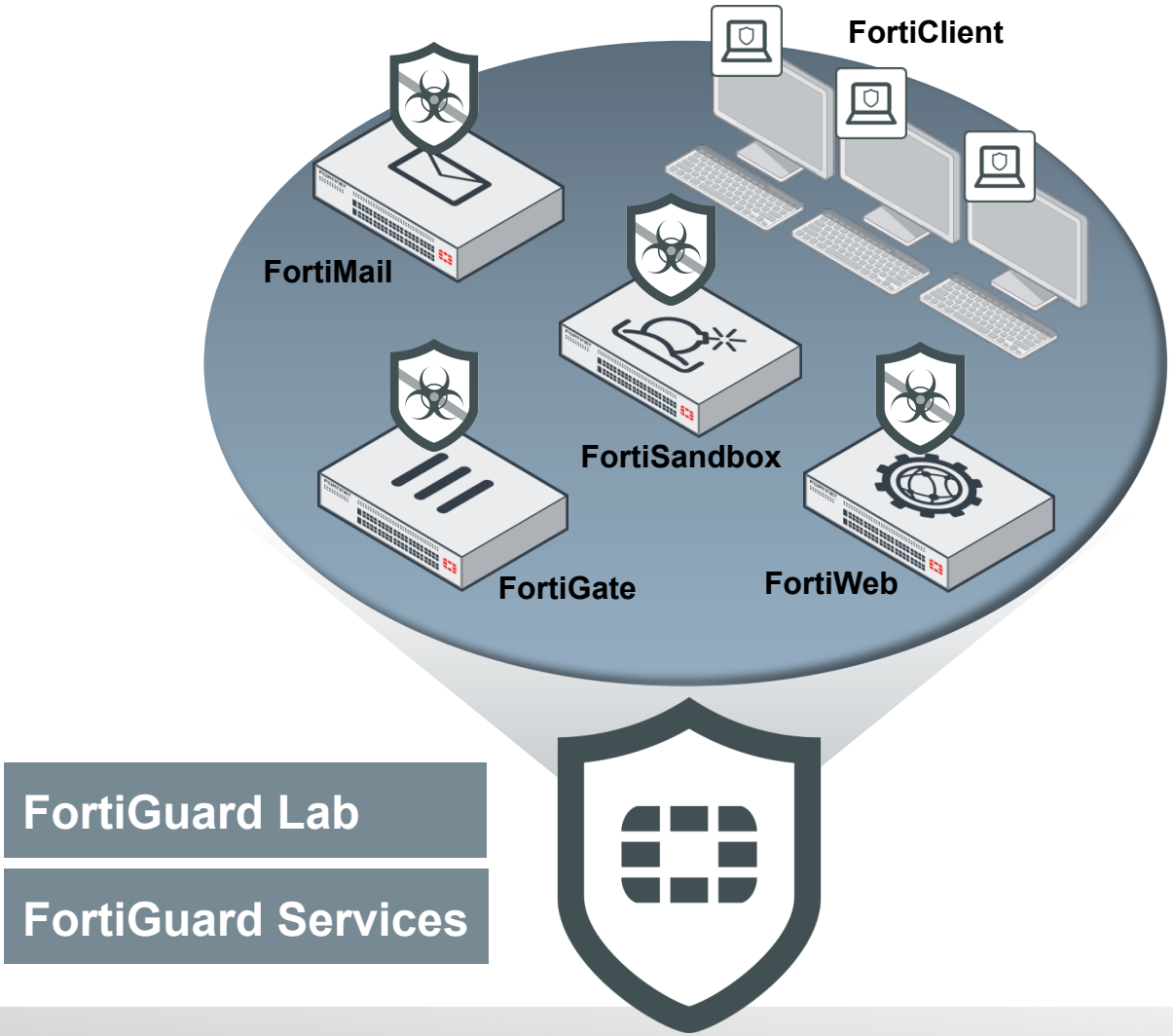


Botnet Detection
IP & Client Reputation
Sandboxing

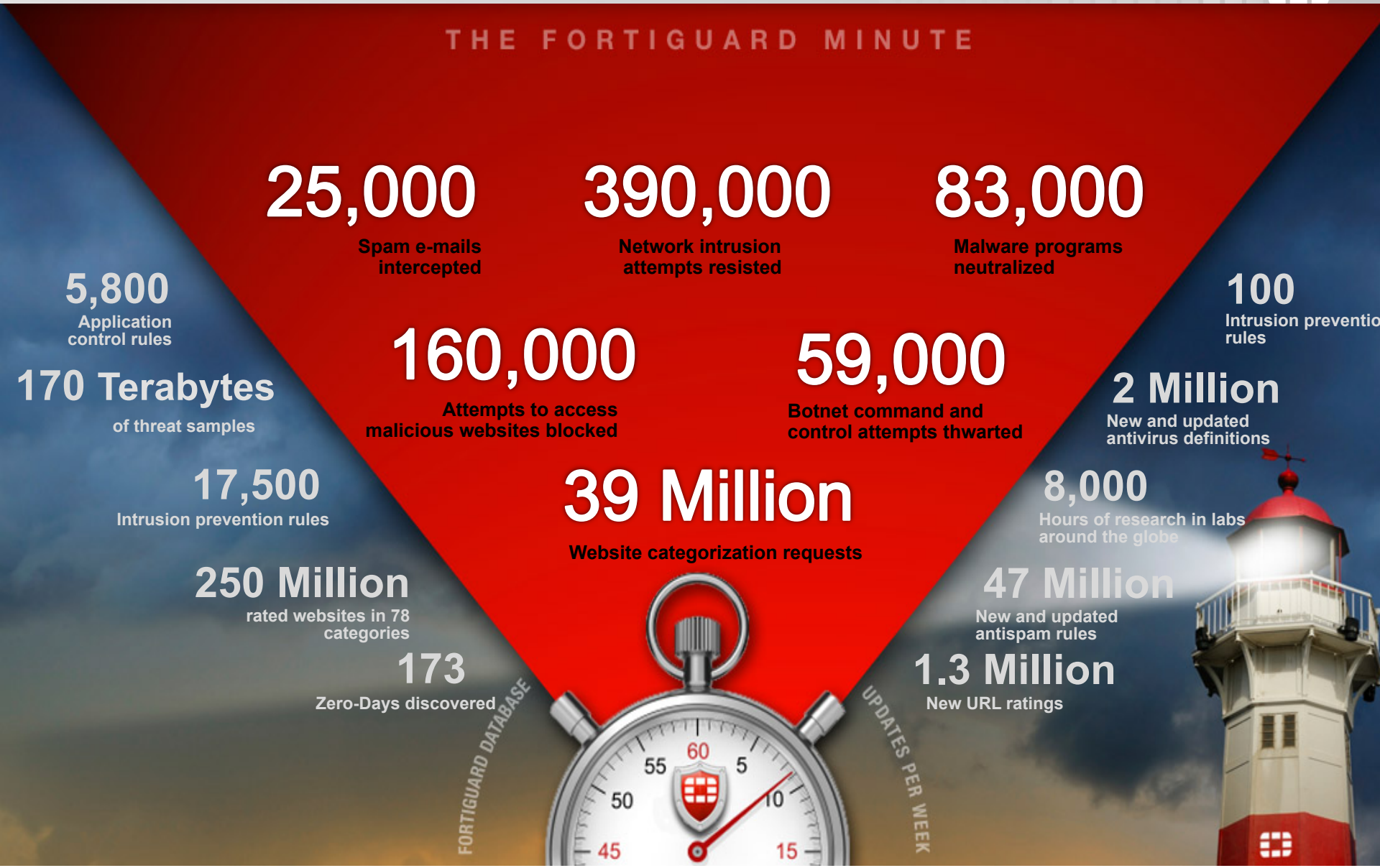
People
Process
Technology

Threat Intelligence
Zero Day Research
Continuous updates

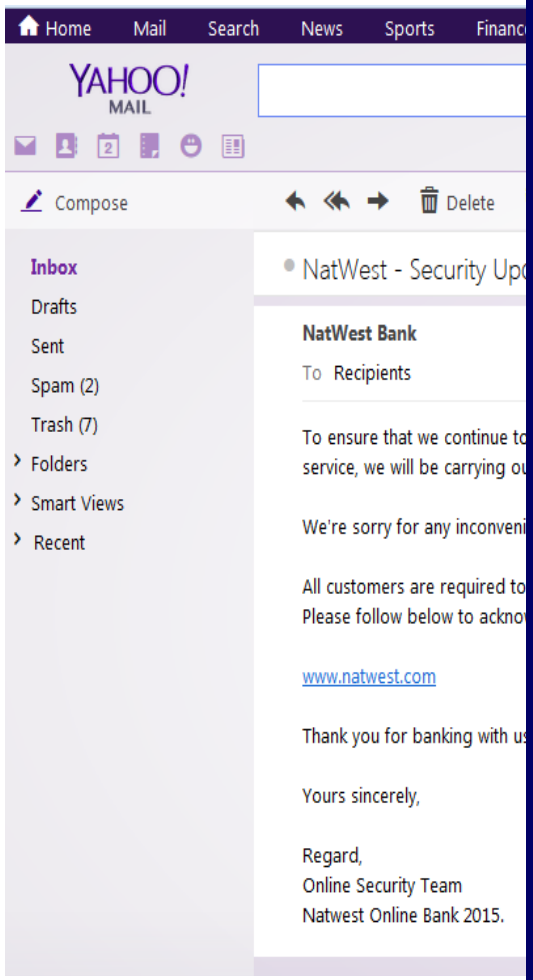
Advanced Threat Protection



The FortiGuard Minute



So What Do We Do With Dave?



Date: Thu, 15 Jan 2015 15:07:19 +0100
From: "Internal Revenue Service" <complaints@irs.gov>
To: <rpastore@cxo.com>
Subject: Complaint against your company

Dear business owner,

A criminal complaint has been filled against your company.

Your company is being accused of trying to commit tax evasion schemes.

The full text of the complaint file (PDF type) can be viewed on the IRS website, by visiting the following link :

http://www.irs.gov/complaints/view_complaint.aspx?complaint_id=931998&hash=329yt8dhui8g14

An official response from your part is required, in order to take further action.

Please review the charges brought forward in the complaint file, and contact us as soon as possible by :

Telephone Assistance for Businesses:
Toll-Free, 1-800-829-4933

Email: complaints@irs.gov

Thank you,

Internal Revenue Service

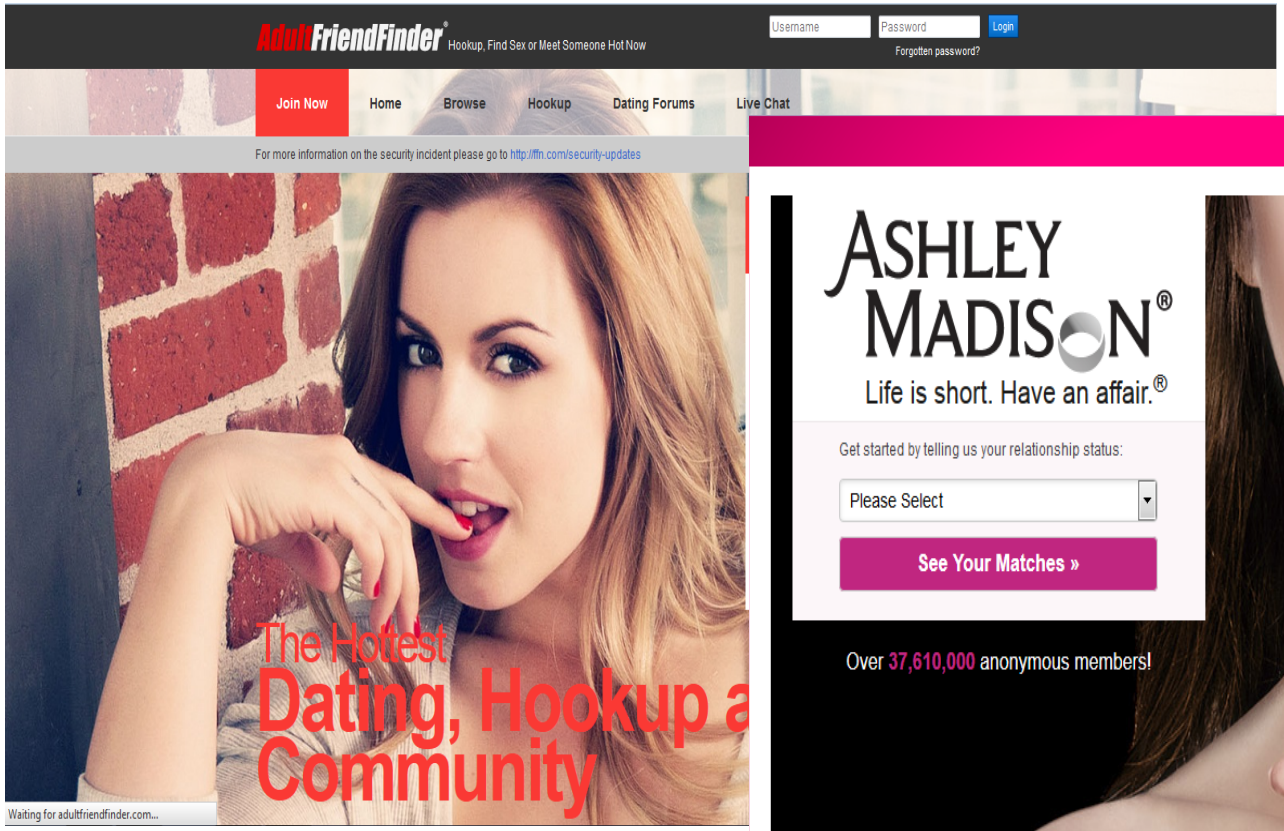
Fraud Prevention Department

Training To Raise Awareness

http://krebsonsecurity.com/2012/01/phishing-your-employees-101/

- Policy
- Procedure
- Process

And At the Opposite End of the Spectrum…



Looking Forward

- ✓ Technology is only part of the solution
- ✓ Single vendor solutions may provide an advantage
  - ✓ But only if elements actually work together
- ✓ Remember your network extends beyond you
  - ✓ Remote employees, third party suppliers and contractors
- ✓ Your employees are the first line of defense
  - ✓ Equip and use them
- ✓ Never assume
  - ✓ You're fully protected
  - ✓ The network hasn't already been breached

Understanding the Data Breaches of 2014: Did it have to be this way?

Vielen Dank!