Learning From The Largest, Most Significant Breaches

Ryan McArthur, MSIA
email: ryan.mcarthur@isc2mainechapter.org

About Me

- Technologist
- Security Professional
- Educator
- Husband, parent, and grandparent
- BS Information Technology
- MS Information Assurance

- Since the mid 1980's
  - TI 99/4A
  - Z80 / IBM XT
  - Honeywell 6 & IBM System 34
- Help Desk
- Programming and Design
- Database Administration
- Continuity
- Cybersecurity
- Information Technology Adjunct Professor

Objective

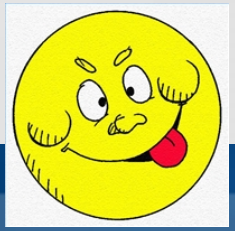
- Examine and understand how world's largest and most impactful data breaches occurred
- Learn from their experiences

Disclaimer

The material in this presentation is based solely upon articles from the Internet, such as professional trade association journals (i.e. ComputerWorld) or national news organizations (New York Times). I am not speaking on behalf of any employer or organization for which I am Director or Officer.

Question

- How many security professionals does it take to change a lightbulb?
  - 3 people for preliminary discussion
  - 4 people to argue about ISO vs NIST, CoBIT, and other applicable standards and best practices
  - 3 people to perform a risk assessment
  - 5 people to write the report
  - 1 person to scare everyone in the room with report
  - Oh and the lightbulb, it's a hardware problem.



- CSO serves Chief Security Officers across the nation with the latest news and insights from industry experts

- CSO profiled the 16 biggest data breaches

Yahoo

- Multiple occasions – all 3 billion user accounts
  - Email addresses
  - Dates of birth
  - Telephone numbers (for 500 million people)
  - Security Questions and their answers

  - Attack Vector: Not disclosed

Adult Friend Finder

- October 2016 – 412.2 million user accounts
  - Adult content website
  - Names
  - Email addresses
  - Passwords

- Attack vector: software vulnerability & weak encryption

eBay

- May 2014
  - 145 million user accounts
  - Names
  - Addresses
  - Dates of birth
  - Passwords

- Attack vector: stolen user credentials for 3 employees giving attackers complete access for 229 days

Heartland Payment Systems

- March 2008 – 135 million credit cards

- Attack vector: SQL Injection – inserting computer logic into a data field.
  - Not in compliance with Payment Card Industry (PCI) standards

TJX Companies, Inc

- December 2006 – 94 million credit cards
- Attack Vector: two plausible methods
  - Weak data encryption in wireless data transfer
  - Brute force through in-store kiosks

JP Morgan Chase

- July 2014 – 76 million households & 7 million businesses
  - Names
  - Addresses
  - Phone numbers
  - Email addresses
  - Internal information about customers

- Attack Vector: Not disclosed
  - Attackers gained “root” privileges (highest level privileges on a system)

US Office of Personnel Management (OPM)

- Circa 2012-2014 – 22 million employee records
  - Employee personal data
  - Detailed security clearance information
  - Fingerprint data
  - SF-86 form (lists every place the employee has lived, traveled, siblings, and children information)

  - Attack Vector: Not disclosed

Sony Playstation

- April 2011 – 77 million accounts hacked
  - 12 million unencrypted credit card numbers
  - Names
  - Passwords
  - Emails addresses
  - Address
  - Purchase history
- Attack Vector: Not disclosed

Anthem

- February 2015 – 78.8 million customers
  - Names
  - Addresses
  - Social Security Numbers
  - Dates of births
  - Employment history
  - Credit card information
  - Medical information

- Attack Vector: Not disclosed

RSA Security

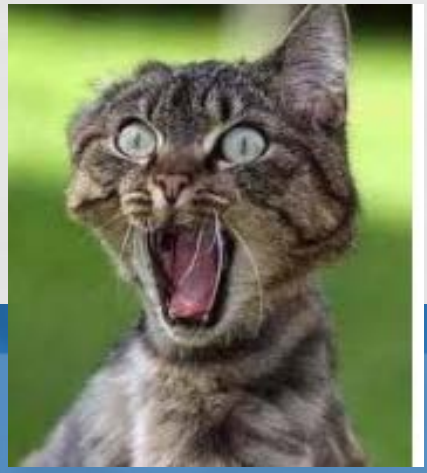
- March 2011 – possibly 40 million employee records stolen
  - Information related to SecurID authentication tokens
- Attack Vector: Phishing attacks
- Positive Outcome: Demonstrated everyone can be vulnerable

Stuxnet

- 2008 – Attack Iran's nuclear power program
  - World’s First Digital Weapon
    - Power grids
    - Water supplies
    - Public transportation systems

VeriSign

- 2010 – Undisclosed information stolen
  - Attackers gained access to privileged systems & information
- Attack Vector: Not disclosed
- As PCWorld put it, “VeriSign buried the information in a quarterly Securities and Exchange Commission (SEC) filing as if it was just another mundane tidbit.”



Home Depot

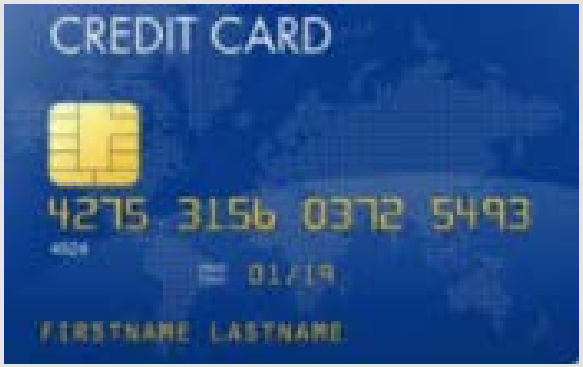
- September 2014 – 56 million credit/debit cards
  - POS systems infected with malware

- Attack Vector: Phishing; malware posing as anti-virus software

Adobe

- October 2013 – 38 million user records
  - Credit numbers
  - User credentials – user IDs and passwords
  - Customer names

- Attack Vector: Not disclosed



Target

- December 2013 – up to 100 million people
  - 40 million credit / debit card numbers stolen
  - 70 million private data records
- Attack Vector: HVAC vendor
  - Stolen user credentials
  - Phishing

- Watershed Moment
  - CEO's, CIOs, CISOs are more accountable
  - Chip and Pin
  - Vendor Management
  - System & Network Segmentation

Equifax

- July 2017 – 143 million consumers
  - Social Security Numbers
  - Birth dates
  - Addresses
  - Drivers' license numbers
  - Credit card data (209,000 consumers)
  - Data for 400,000 British 100,000 Canadian consumers

  - Attack Vector: Unpatched Apache Struts
    - Multiple websites w/ vulnerabilities

Equifax

- Why is this breach so bad?
  - Treasure chest consumer private information
  - Major data aggregator, broker, and analytics firm
  - Consumers most private financial information

- What we know
  - CVE-2017-5638 – exploiting this is documented
  - Easy to exploit
  - Web application tricked into executing O/S Commands
  - Attacker *owned* the system within minutes

Equifax

- SQL Injection easy to accomplish

```
SELECT *
  FROM customer-credit-file
```

Equifax

- Business problems
  - 40 days to report
  - CFO sold $1.8 million of stock options the day after discovery
  - Sale of stock approved by Chief Legal Officer
- Terminations
  - CEO
  - CIO
  - CISO

Equifax

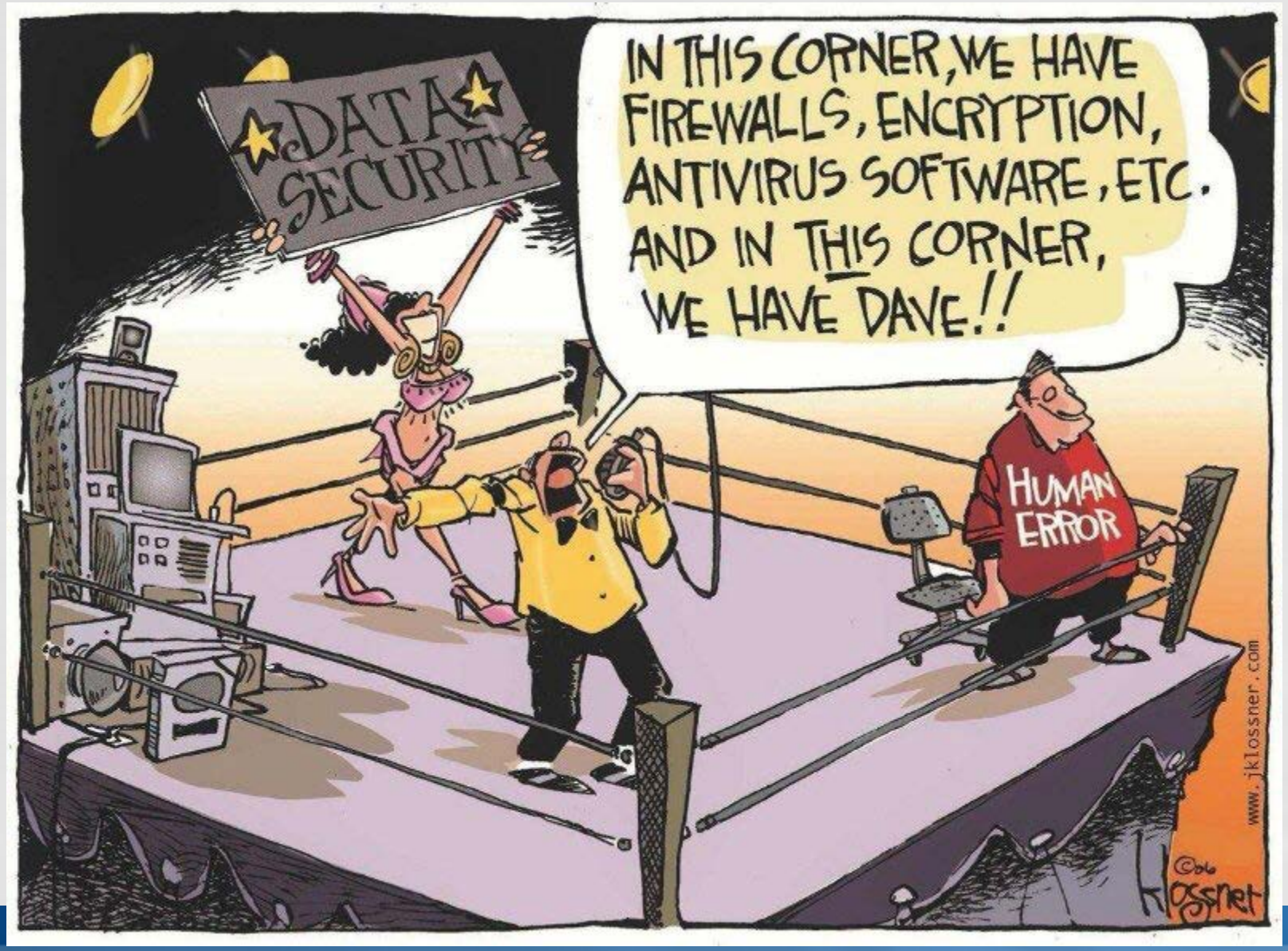
- Watershed Moment
  - Patching Standards & compliance review
  - Detection, Response, and Notification
  - Corporate Officer Responsibilities

Similarities

- Password Management
- Phishing
- Software Vulnerability – patching

- Security Program
  - Policies & Procedures
  - Password standards – complexity and changing
  - End user training
  - Risk Assessments
  - Compliance Review

- Human Error


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

Wow!

- Companies were heavily investing in companies
- Lot of software, staff, and consultants
- Companies were spending tons of money
  - At the time of the breach, JP Morgan was spending $250 million per year

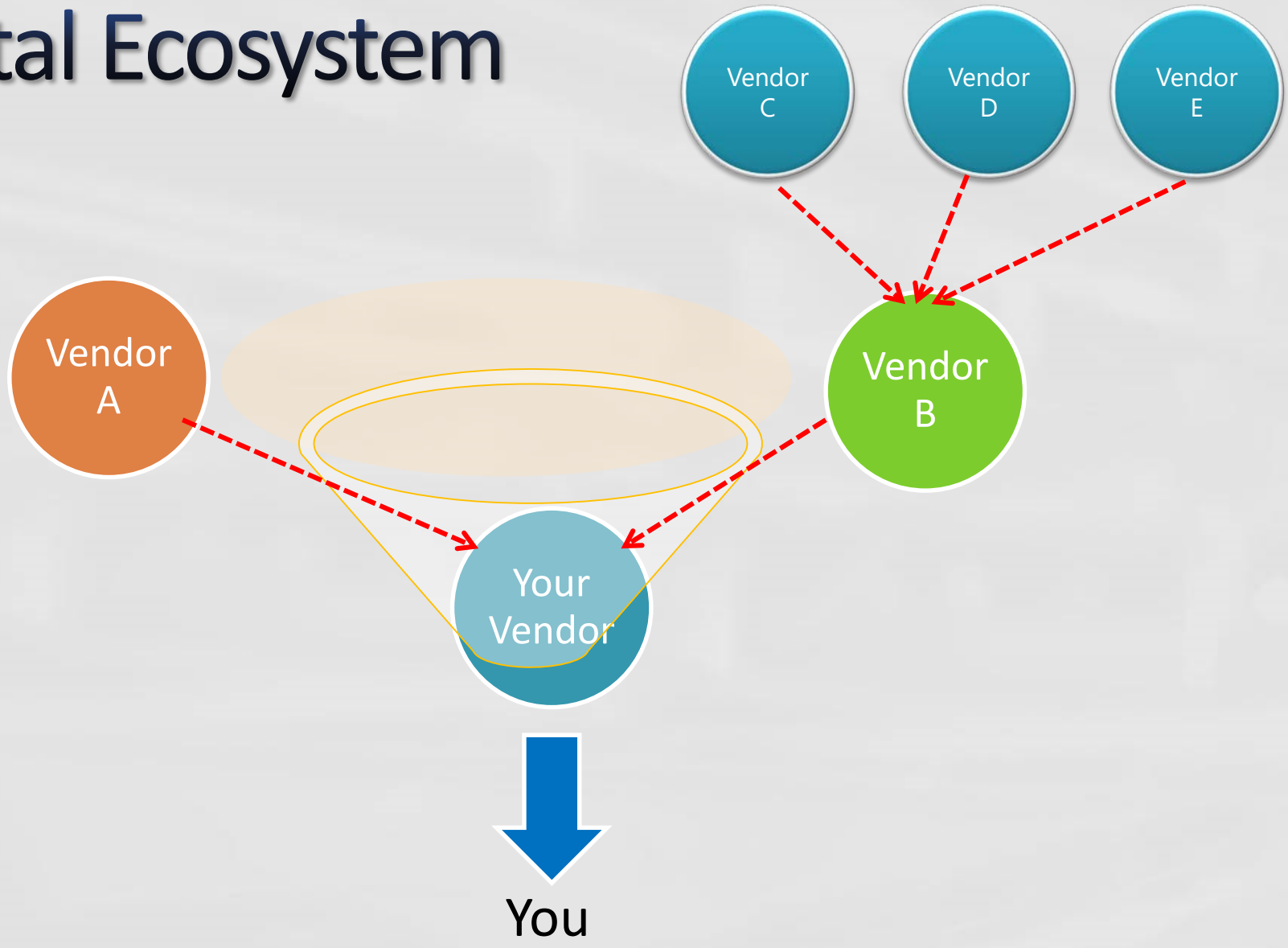
Making sure you do not become a victim

Adapt to Survive and Thrive

Avoiding being in the bulleye's – build a wall

- Policy documents
- Know thy vendor
- Perimeter
- Internal networks
- Network and controls
- Training
- Organizational Structure
- Compliance verification

Digital Ecosystem



How well do you know your vendors?

- Conduct a Risk Assessment against vendor
  - Risks within organization's risk tolerance
- Vendor's security program
  - Security policies and procedures
  - Security training for vendor's employees
  - Who has access to the vendor's network
  - How / where does the vendor keep YOUR passwords
    - Who has access to YOUR passwords
  - What do you know about your vendor's vendors

How do vendors access your network?

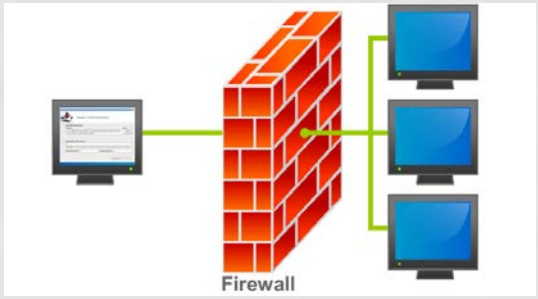
- VPN, 2-factor authentication, etc.
- Monitor vendor portal access
  - Process to identify anomalies
- Menu or command prompt interface
- Use of privileged accounts
- Separate accounts for
  - Devices
  - Servers
  - Applications, files, and databases

Contractual Requirements for Vendor

- Require vendor to tell you if they have a breach
- Provide copy of SSAE16 SOC 1 / 2 report
- Use commercially available AV program
  - No freebies
  - Software and definitions kept up-to-date
- Patch Management
- Security provisions extended beyond contract's term
- Data returns to you after contract termination

Network and Perimeter Security

- Use Two Factor Authentication
  - Secure ID / Smartphone App
  - Multiple questions
  - SMS Messaging



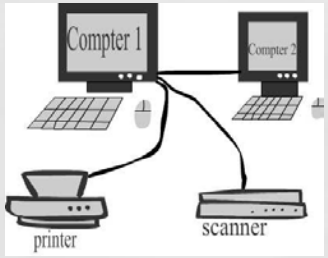
- Network segmentation
- Limit network access to systems containing critical business systems / data
  - Access on an “as needed” basis
  - Privileges align with tasks being performed
  - Separation of duties

Accounts & Passwords

- Using best practices
  - Minimum length
  - Complex and Aging
- Scrutinize privilege accounts
- Change from default password values
- Disable/remove unused or unnecessary accounts

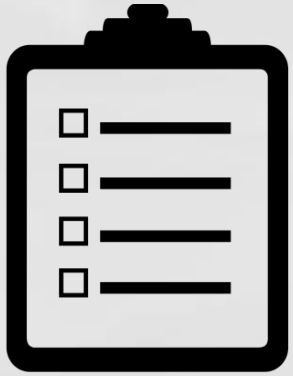
Inside the Perimeter

- Non-production systems with data need to be secure too or remove the data!
- Internal network scanning
  - Intensive review of passwords, software, etc.
  - Planned and unannounced
  - Formal independent testing annually
- Detection of file creation and movement
- Detection of file transmissions
  - Data Loss Prevention (DLP) tools



Inventory of approved software

- Purchase – Commercial Off the Shelf (COTS)
- Open Source
- Internally built programs – standards
- Whitelisting applications / programs
- Cloud – know who own's the data and where the data resides



Controls

- Change Management System
  - Monitoring software installation
  - Review changes
  - Software versions / Patches
- Useful Common Controls
  - Limit Administrator / Domain Admin privileges
  - Remove unnecessary software
  - Run apps in Virtual Environment for the first time
- Block first – ask questions later
  - Automatically block or delete suspicious software
  - Don’t assume false positive – assume it is a legitimate threat until **PROVEN** otherwise
- Incident Response Plan

Policies and Employees

- Are your policies followed by employees and vendors?
  - How do you know?

- Clearly communicated security objectives and outcomes from the top
- My IT staff understands the organization's security expectations?
  - Do you really know?
  - How do you validate?

Culture and Employees

- Escalation of alerts / concerns
  - Reporting
  - Decision making
  - Action taken
  - Closure and documentation
- Formal testing and drills
  - Planned and unannounced
  - Includes internal software, systems, and devices
  - Lessons learned and documentation updates

Common Excuses by employees

- Too busy
- Too few people
- Too few dollars
- Too complex … we are too small
- Not necessary … we are not the focus of attackers

- But yet, everyone could become the focus of an attacker if you have money or useful data

Simple changes can make a difference

Quote from Target

"Ensure the right people, with the right experience, with the right education and certifications, are in the right position to protect the network and data"

Target press release