Houston
Financial
Forensics

Forensic Accounting Services

# Cyberfraud in 2017

## ACFE – North Houston

## Dan Ramey, CPA, CFE, CFF, CISA

## November 30, 2017

Houston Financial Forensics
Forensic Accounting Services

# Dan Ramey, CPA/CFF/CITP/ABV, CFE, CVA, CIA/CRMA, CISA/CISM and CMA

***Dan Ramey*** *is the Founder and President of Houston Financial Forensics, LLC and Dan T. Ramey, CPA, LLC.  Dan was formerly the Director of Risk Advisory Services for RSM (McGladrey) LLP in Houston, Texas.  Dan's professional certifications include: CPA/CFF/CITP/ABV, CFE, CVA, CIA/CRMA, CISA/CISM, and CMA.  He is a past President of the Houston Chapter of the Institute of Internal Auditors and formerly a member of the Board of Governors.  Dan previously served as Chairman of the Houston CPA Society's Forensic and Valuation Committee and as Treasurer of the Houston Chapter of InfraGard.  He is also active the Houston FENG Chapter where he was held several leadership roles.  Dan is a Lifetime Member of the Greater Houston Partnership where he served for several years on the Ally Committee integrating new members into the organization.  Dan teaches graduate level Fraud Examination and Enterprise Risk Management classes at the Bauer School of Business at the University of Houston.*

*Dan is also a frequent speaker to business and professional groups on fraud, risk assessment, third-party risk management, cybersecurity, fraudulent financial reporting, internal audit, COSO 2013, valuation methodology, and due diligence.  Dan is a graduate of Baylor University with a degree in Accounting and an Executive MBA from Houston Baptist University.  He is a member of Second Baptist Church where he serves as a Deacon.  Dan also serves on the Houston Baptist University Business School Dean's Development Council and the Accounting Advisory Board at Bauer College of Business at the University of Houston where he also serves as the Chair of the Outreach Committee.*

*Houston Financial Forensics, LLP and Dan T. Ramey, CPA, LLP are premier providers of forensic accounting and risk management services to corporate, professional services, and non-profit clients.*

# Houston Financial Forensics, LLC

Houston Financial Forensics, LLC is a provider of professional services to corporations, nonprofits, and professional service firms in the areas of internal audit, fraud investigation, enterprise and cyber / IT risk assessment, fraud risk assessment, internal controls, forensic accounting, business valuation, litigation support, Sarbanes-Oxley 404, internal audit department quality assessment reviews, third-party risk management, and due diligence for mergers and acquisitions.

*Houston Financial Forensics is not a CPA firm.*

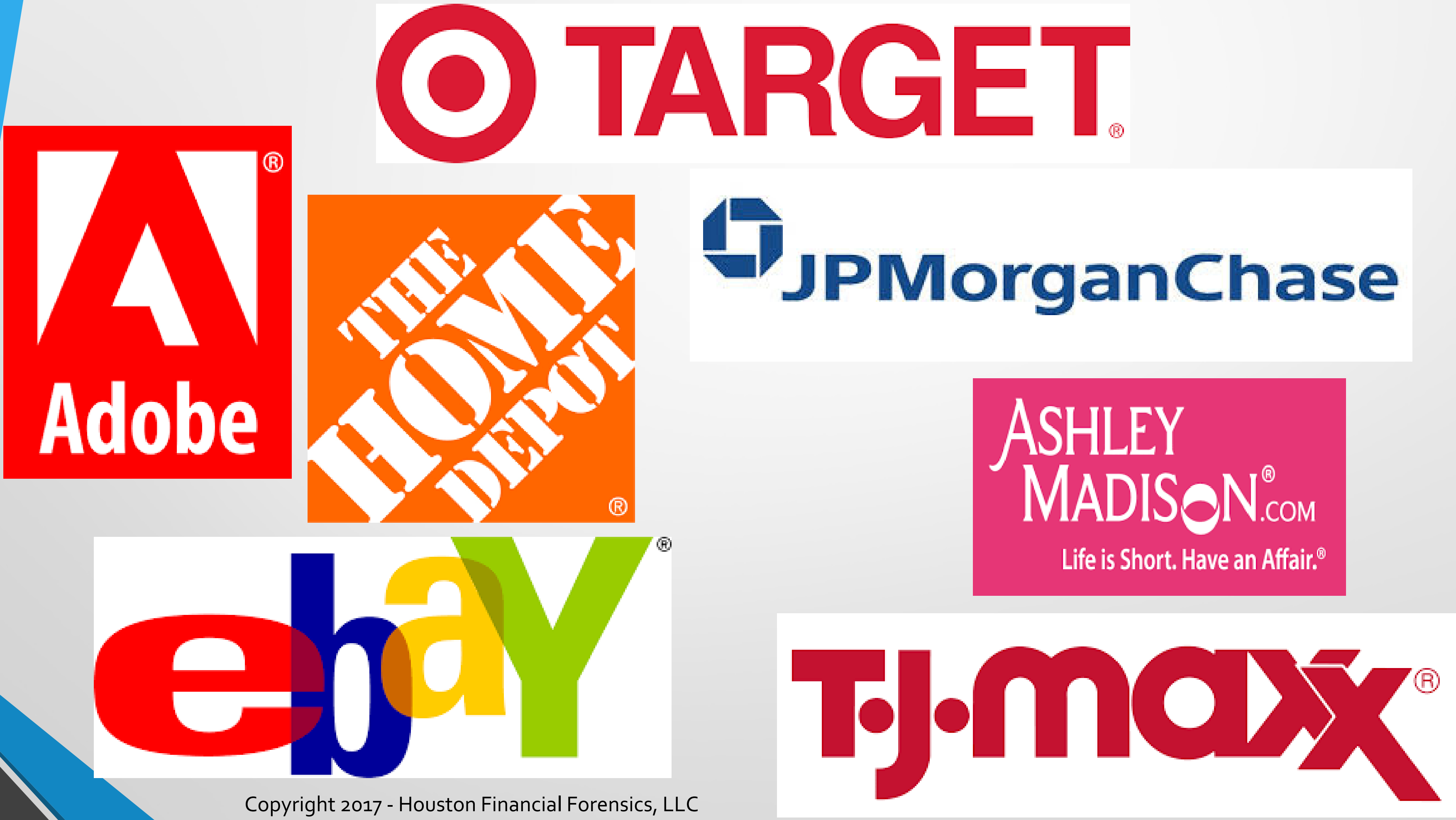
# Data Has Value

# Organizational / Culture Change

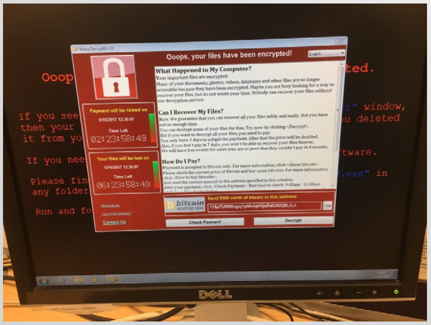
VS

# Cyber Security and Compliance

# Cyber Fraud - 2016



# Cyber Fraud – 2017



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49

Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49

About bitcoin
How to buy bitcoins?
Contact Us

bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy

Check Payment
Decrypt

# Cyber Fraud – 2017

| Company | Breach |
|---|---|
| Wendy’s | 300 restaurants |
| **Yahoo** | **3.5 billion accounts and related information** |
| LinkedIn | 286 million email and password combinations |
| Snapchat | 700 current and former employees |
| IRS | 845,950 – 9 breaches |
| DOJ | 10 thousand DHS and 20 thousand FBI agents |
| **Equifax** | **145,950,535 records** |

Source: https://www.privacyrights.org/data-breaches

# Cyber Fraud / Cyber Crime

Any type of deliberate deception for unfair or unlawful gain that occurs online

# Who Are the Hackers?

- Nation – States
- Hacktivists
- Organized Crime Syndicates
- **Insiders**

# Cyber Fraud Statistics

- 75% of breaches were perpetrated by outsiders
- 25% of breaches were perpetrated by insiders
- 18% of breaches were by state-affiliated actors
- 51% of the breaches include malware
- 81% of breaches used stolen and/or weak passwords
- 73% of breaches were financially motivated
- 21% of breaches were related to espionage
- 95% of phishing attacks that lead to a breach were followed by some type of software installation

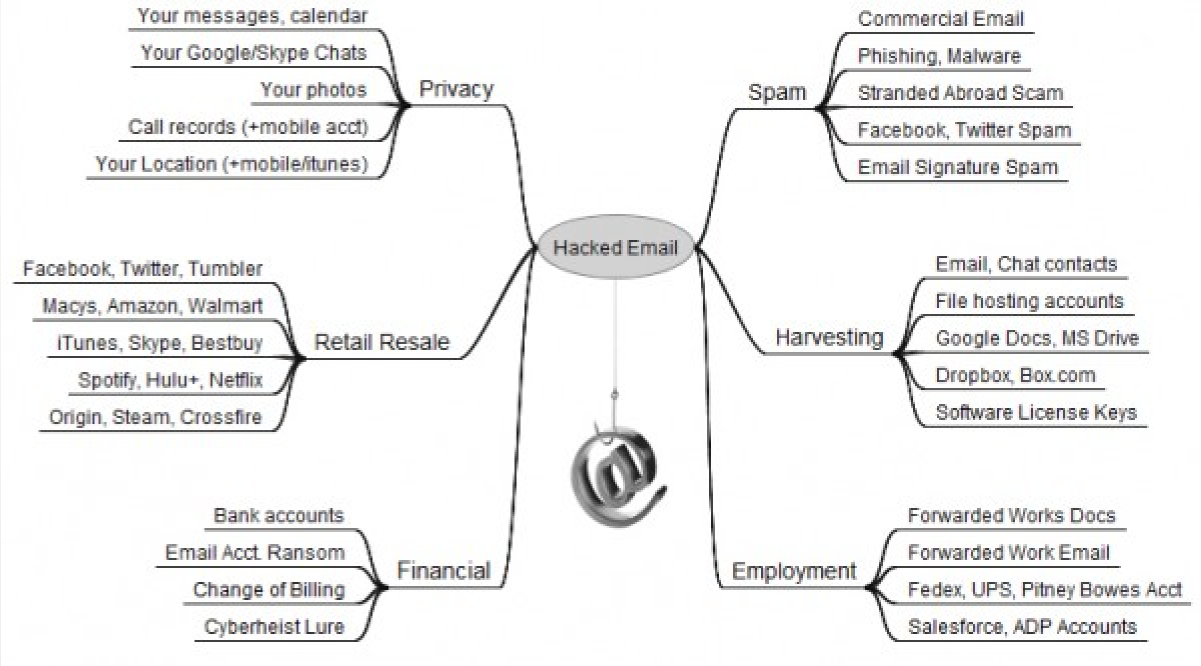
*Source: Verizon Data Breach Investigations Report - 2017*

# Data Breaches – 2013-2017

| Category | Breaches | Records Accessed |
|---|---|---|
| 2017 | 522 | 1.9 **Billion** |
| 2016 | 807 | 11 Million |
| 2015 | 531 | 160 Million |
| 2014 | 575 | 68 Million |
| 2013 | 885 | 61 Million |

Source:  Privacy Rights Clearinghouse

# Hacked Email Account Value



Source: https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

# Categories of Cyber Crimes

- Computer Break-Ins
- Phishing Attacks
- Whaling
- Business Email Compromise (BEC)
- Malware / Ransomware
- Distributed Denial of Service
- Child Pornography

# Personally Identifiable Information (PII)

Personally identifiable information (**PII**) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered **PII**.

- Sensitive PII
- Non-Sensitive PII

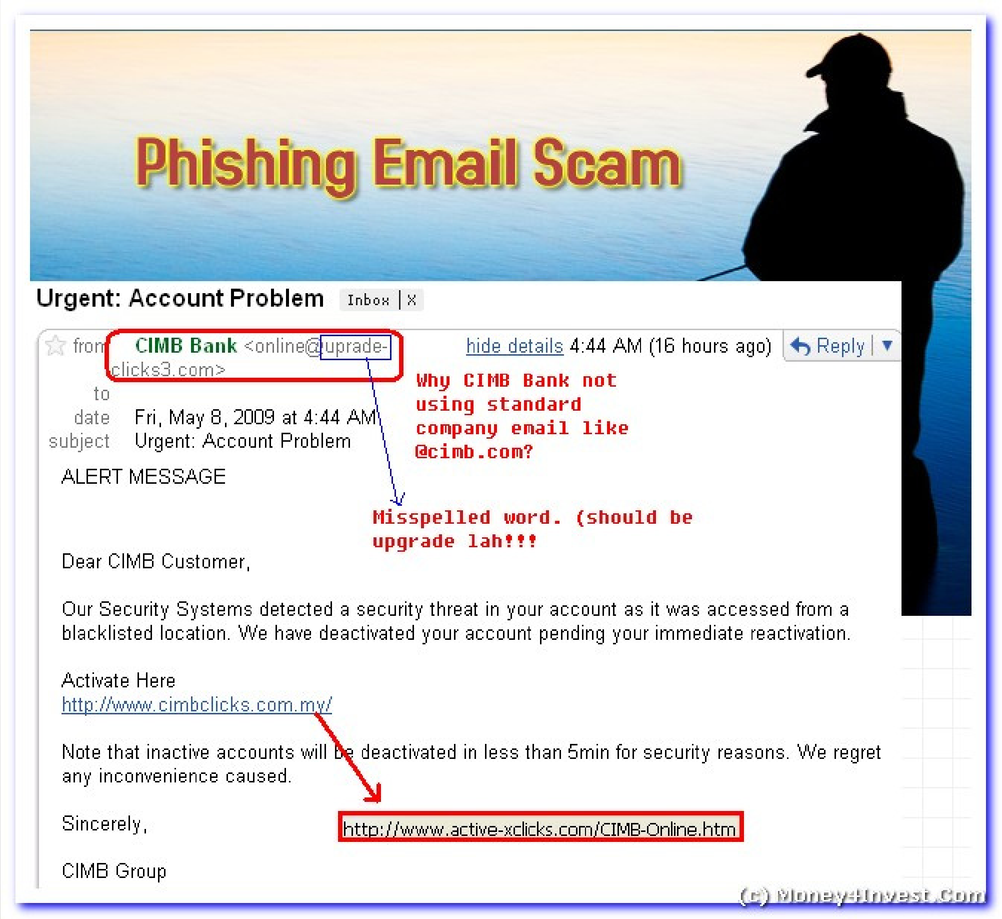
# Non-Sensitive PII

- Name
- Work and Personal Email Address
- Home and Work Addresses
- Business Phone Number
- Work and Personal Cell Phone Numbers

# Sensitive PII

- Ethnicity / Race
- ID Number (Social Security / Passport)
- Employment History
- Date of Birth / Place of Birth
- Medical History / Medical Conditions
- Financial Accounts
- Drivers License Number
- Mother’s Maiden Name

# Phishing Email Example



Urgent: Account Problem Inbox | X

from CIMB Bank <online@uprade-clicks3.com>
to
date Fri, May 8, 2009 at 4:44 AM
subject Urgent: Account Problem

hide details 4:44 AM (16 hours ago) Reply

Why CIMB Bank not using standard company email like @cimb.com?

Misspelled word. (should be upgrade lah!!!

ALERT MESSAGE

Dear CIMB Customer,

Our Security Systems detected a security threat in your account as it was accessed from a blacklisted location. We have deactivated your account pending your immediate reactivation.

Activate Here
http://www.cimbclicks.com.my/

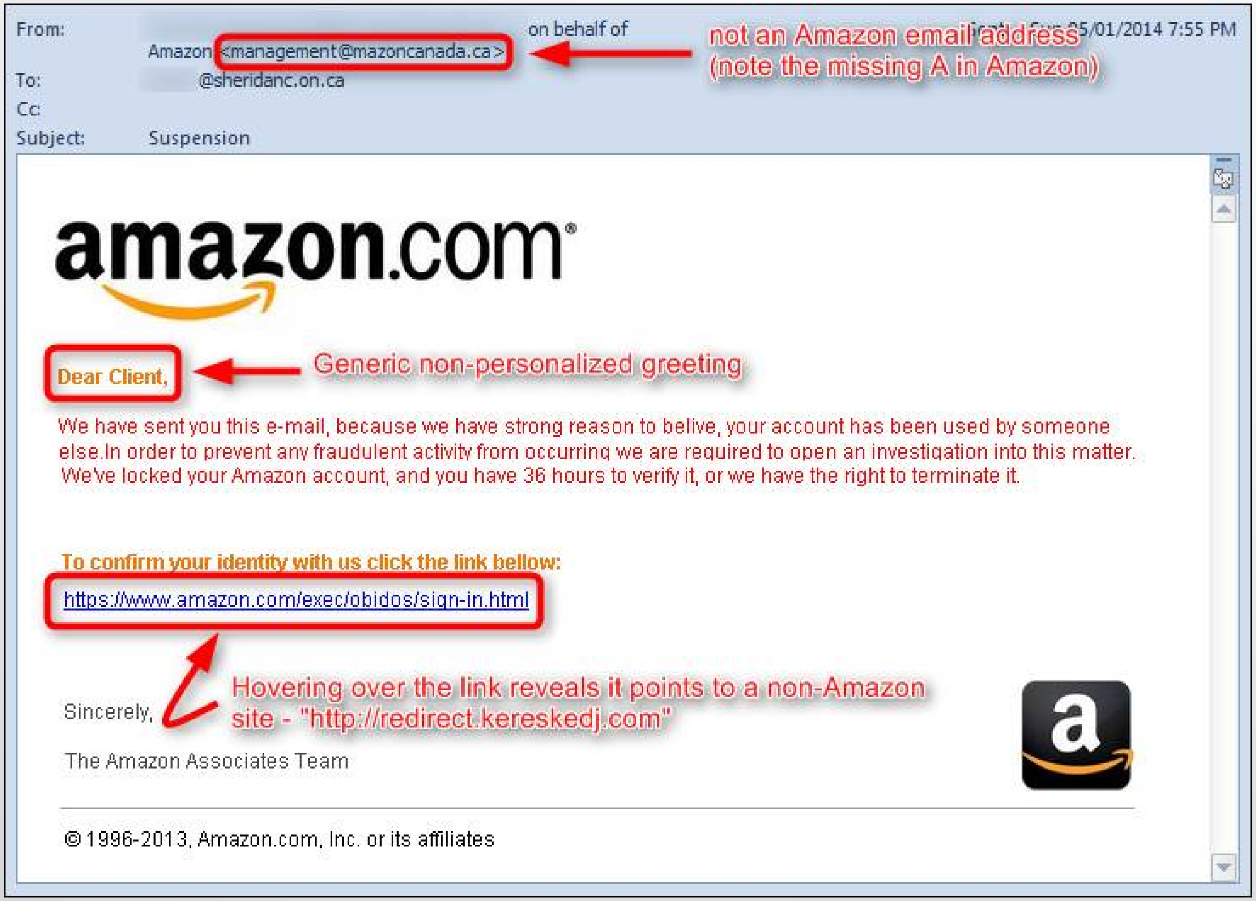
http://www.active-xclicks.com/CIMB-Online.htm

Note that inactive accounts will be deactivated in less than 5min for security reasons. We regret any inconvenience caused.

Sincerely,

CIMB Group

# Phishing Email Example



From: [redacted] on behalf of Amazon <management@mazoncanada.ca>

05/01/2014 7:55 PM

To: [redacted]@sheridanc.on.ca

Cc:

Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

Copyright 2017 - Houston Financial Forensics, LLC

# Business Email Compromise (BEC)

- Also known as "CEO Fraud"
- The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.
- Examples
  - **Ubiquiti Networks Inc.** - $46.7 million
  - **The Scoular Co** - $17.2 million

# Business Email Compromise (BEC)

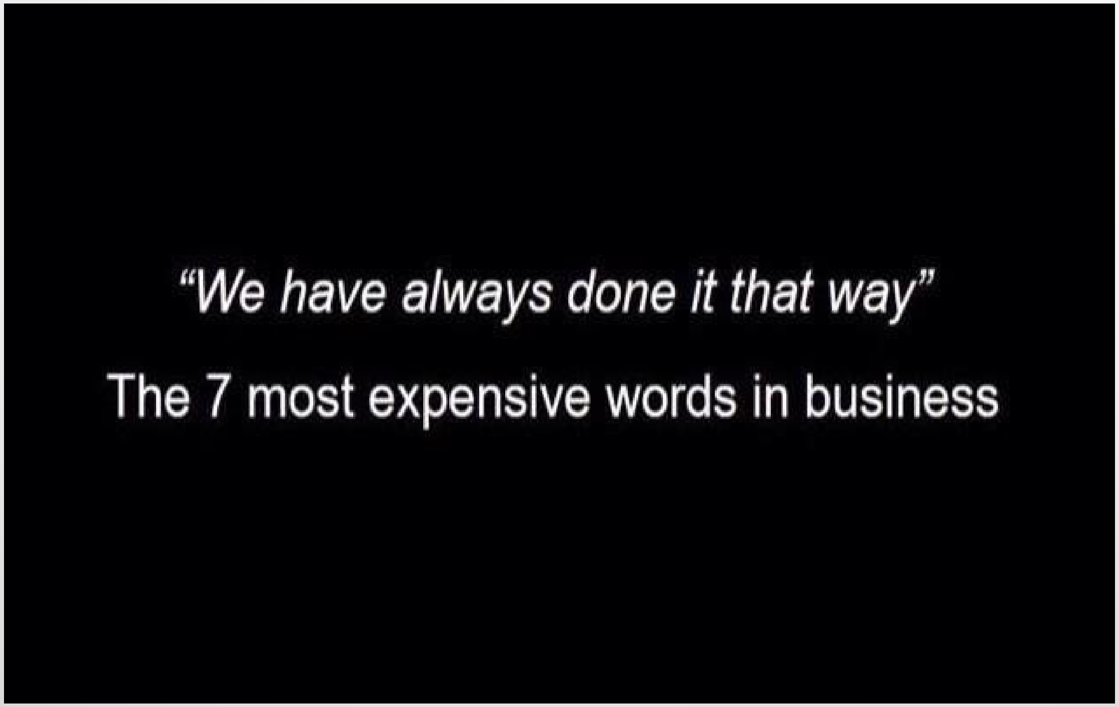
| **October 2013 to December 2016 (multiple sources of data)** | |
|---|---|
| Domestic and international incidents: | 40,203 |
| Domestic and international exposed dollar loss: | **$5,302,890,448** |

The following BEC/EAC statistics were reported in victim complaints to the IC3from **October 2013 to December 2016:**

| | |
|---|---|
| Total U.S. victims: | 22,292 |
| Total U.S. exposed dollar loss: | $1,594,503,669 |
| Total non-U.S. victims: | 2,053 |
| Total non-U.S. exposed dollar loss: | $626,915,475 |

Source: https://www.ic3.gov/media/2017/170504.aspx

# “We have………..”



*“We have always done it that way”*

The 7 most expensive words in business

# NIST 800.53 – Cyber Security Framework

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

# AICPA – Cyber Security Risk Management Framework

A cybersecurity risk management reporting framework that assists organizations as they communicate relevant and useful information about the effectiveness of their cybersecurity risk management programs.

# Cyber Security – Best Practices

- Mobile Devices
  - Limit access to work materials on approved devices
  - Use secured networks when accessing work materials on personal devices
  - Protect access with passwords
  - Do not use public Wifi (i.e. Starbucks, etc.)
  - Use VPN connection if public Wifi is used

# Cyber Security – Best Practices

- Employee Theft
  - Limit access to sensitive information on a “need to know” basis that’s frequently re-evaluated
  - Monitor employee usage of sensitive information
  - Education
  - Legal agreements in place

# Cyber Security – Best Practices

- Malware and Phishing Emails
  - Train employees not to click on phishing emails or visit suspicious websites
  - Filter access to harmful sites and emails
  - Upgrade to the latest available operating system
  - Maintain and update security software
  - Phish your employees

# Cyber Security – Best Practices

- Third-party Vendors
  - Ensure that subcontractors have vigorous data protection systems in place
  - Monitor ports and open accounts for third-parties
  - Inactivate / close accounts when not in use
  - Limit rights to only data areas required
  - Provide for contractual wording that:
    - Requires specific infrastructure protection
    - Ability to audit prior to contract commencement date
    - Ability to perform audits during the course of the contact
    - Ability to immediately perform an audit when a breach is suspected

# Cyber Security – Best Practices

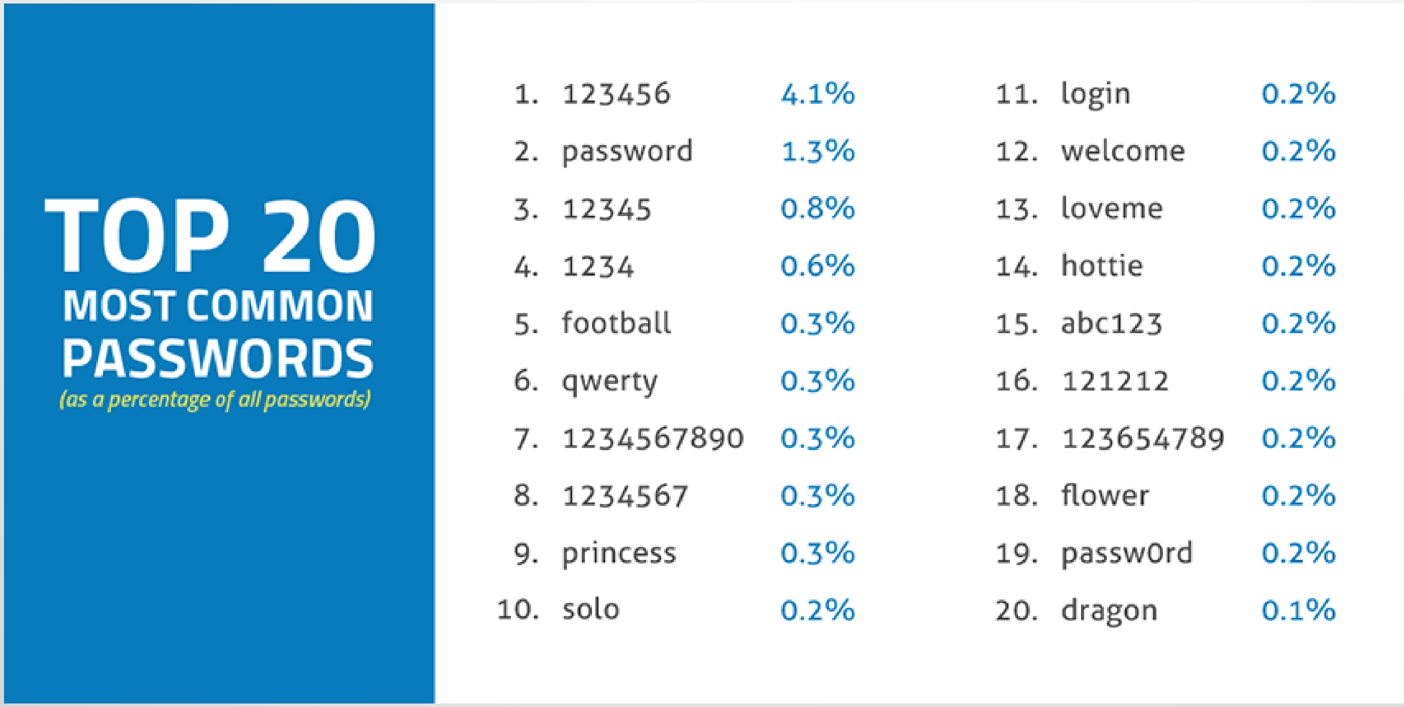
- Software and Hardware
  - Establish controls to prevent unauthorized access to a organization's systems and data
  - Encrypt data to protect it from unauthorized access
  - Perform penetration testing (internal and external) periodically depending on sensitivity of data
  - Keep data and systems backed up – business and personal
  - Keep security software current on all devices
  - Clean browser cache frequently

# Cyber Security Evaluation Tool (CSET)

**CSET** is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems.

- CSET website: https://cset.inl.gov/SitePages/Home.aspx

# Passwords



TOP 20
MOST COMMON PASSWORDS
*(as a percentage of all passwords)*

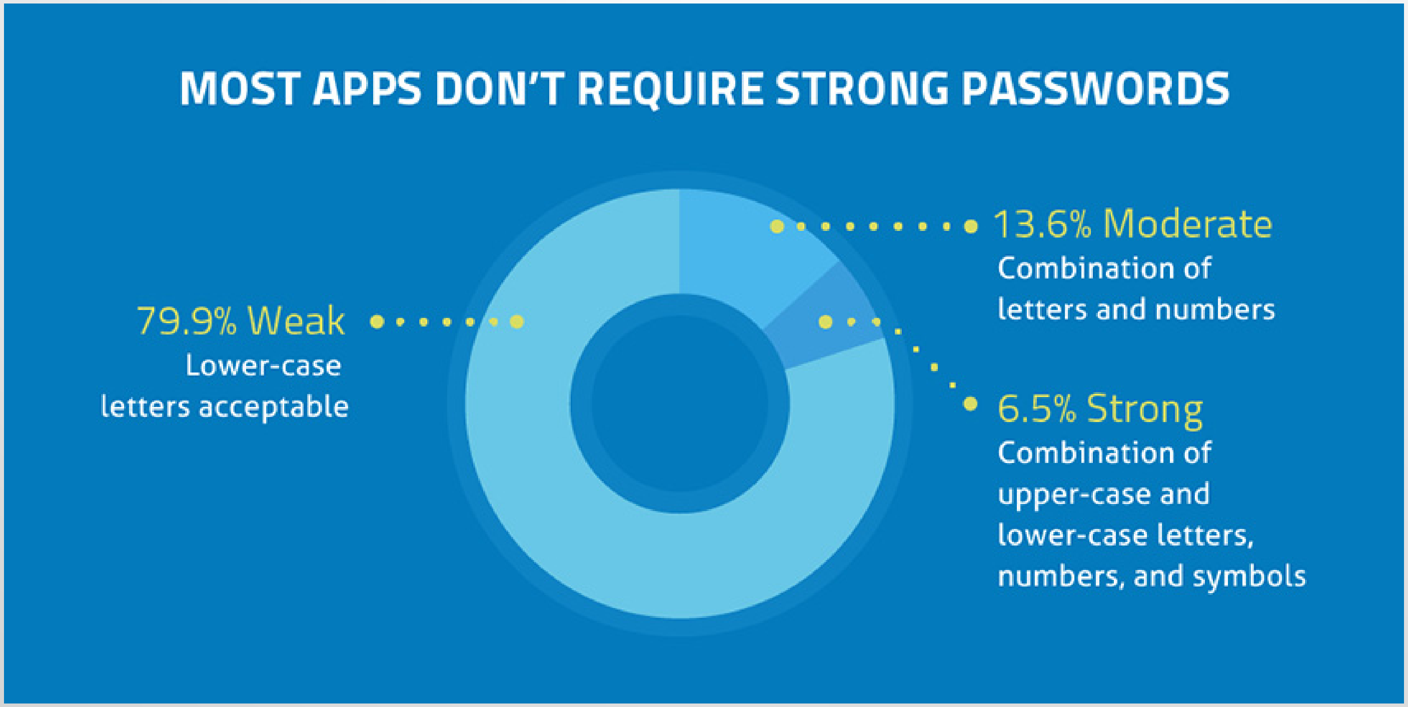
| | | | | | |
|---|---|---|---|---|---|
| 1. | 123456 | 4.1% | 11. | login | 0.2% |
| 2. | password | 1.3% | 12. | welcome | 0.2% |
| 3. | 12345 | 0.8% | 13. | loveme | 0.2% |
| 4. | 1234 | 0.6% | 14. | hottie | 0.2% |
| 5. | football | 0.3% | 15. | abc123 | 0.2% |
| 6. | qwerty | 0.3% | 16. | 121212 | 0.2% |
| 7. | 1234567890 | 0.3% | 17. | 123654789 | 0.2% |
| 8. | 1234567 | 0.3% | 18. | flower | 0.2% |
| 9. | princess | 0.3% | 19. | passw0rd | 0.2% |
| 10. | solo | 0.2% | 20. | dragon | 0.1% |

# Passwords

A recent study of 11 million passwords found that:

- 10.3% of users employ the 20 most popular passwords
- With fewer than 20 tries anyone can log in to roughly 1 out of 10 accounts
- Top password is 123456 and is so common that it makes up 4.1% of all passwords

# Application Requirements for Password



MOST APPS DON'T REQUIRE STRONG PASSWORDS

79.9% Weak
Lower-case
letters acceptable

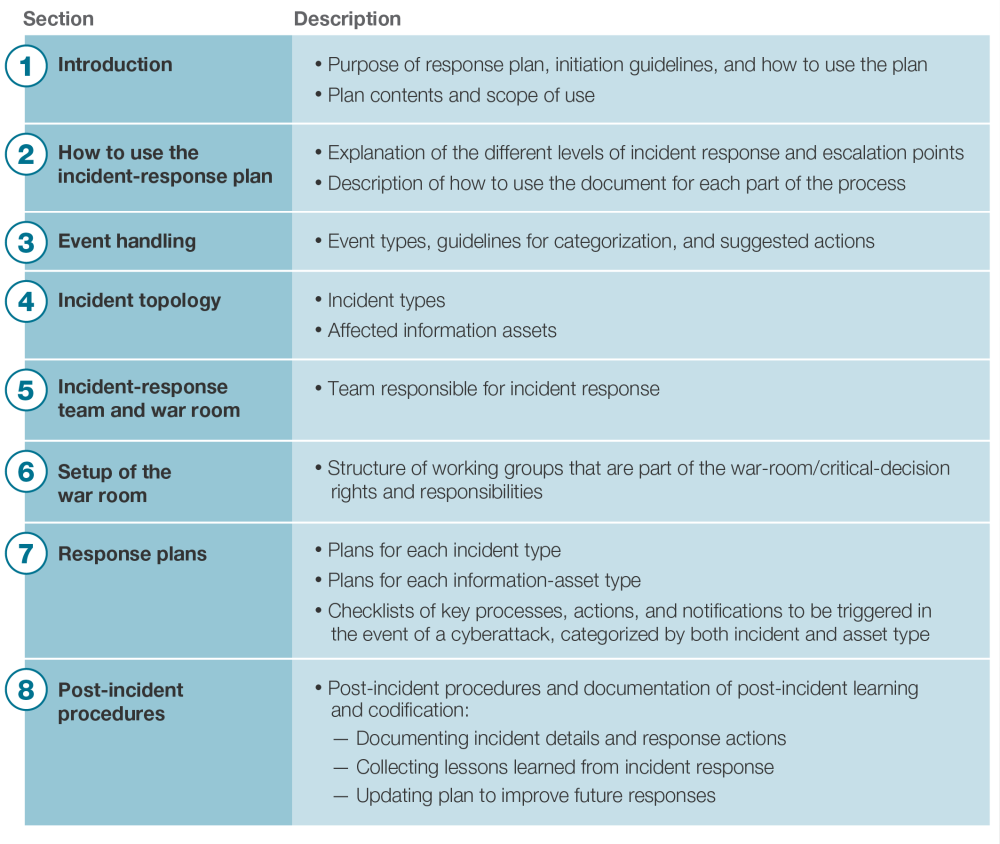
13.6% Moderate
Combination of
letters and numbers

6.5% Strong
Combination of
upper-case and
lower-case letters,
numbers, and symbols

# Password Recommendations

- Minimum Length
  - Mobile devices – 8
  - Networked computers – 8
  - Admins and Privileged Accounts – 10-12
- Password Difficulty
  - Must contain 1 alphabetic, 1 numeric, and 1 symbol character
  - Passphrases
    - Never forgot that your wife’s birthday is on October 23!
    - **Nftyw’bioO23!**
- Password Meter: www.passwordmeter.com

# Incident Response Plan



| Section | Description |
|---|---|
| 1 Introduction | • Purpose of response plan, initiation guidelines, and how to use the plan<br>• Plan contents and scope of use |
| 2 How to use the incident-response plan | • Explanation of the different levels of incident response and escalation points<br>• Description of how to use the document for each part of the process |
| 3 Event handling | • Event types, guidelines for categorization, and suggested actions |
| 4 Incident topology | • Incident types<br>• Affected information assets |
| 5 Incident-response team and war room | • Team responsible for incident response |
| 6 Setup of the war room | • Structure of working groups that are part of the war-room/critical-decision rights and responsibilities |
| 7 Response plans | • Plans for each incident type<br>• Plans for each information-asset type<br>• Checklists of key processes, actions, and notifications to be triggered in the event of a cyberattack, categorized by both incident and asset type |
| 8 Post-incident procedures | • Post-incident procedures and documentation of post-incident learning and codification:<br>— Documenting incident details and response actions<br>— Collecting lessons learned from incident response<br>— Updating plan to improve future responses |

Source: McKinsey and Company

http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/how-good-is-your-cyberincident-response-plan#0

# Cyber Liability Insurance

- **Data breach/privacy crisis management cover**:  Expenses related to the management of an incident, the investigation, the remediation, data subject notification, call management, credit checking for data subjects, legal costs, court attendance and regulatory fines.
- **Multimedia/Media liability cover**:  Third-party damages covered can include specific defacement of website and intellectual property rights infringement.
- **Extortion liability cover**:  Losses due to a threat of extortion, professional fees related to dealing with the extortion.
- **Network security liability**: Third-party damages as a result of denial of access, costs related to data on third-party suppliers and costs related to the theft of data on third-party systems.

Source:  http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover

# Cyber Security and IT Risk Assessment Tools

- IIA GAIT (Guide to the Assessment of IT Risk

http://www.theiia.org/guidance/technology/gait/

- NIST – Cyber Security Framework  based on existing standards, guidelines, and practices

http://www.nist.gov/cyberframework/

# NIST Cyber Security Framework Tools

- Framework for Improving Critical Infrastructure Cybersecurity http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
- Framework for Improving Critical Infrastructure Cybersecurity – Roadmap http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf

# NIST Cyber Security Framework Tools

- Cybersecurity Framework Core – XLS http://www.nist.gov/cyberframework/upload/framework-for-improving-critical-infrastructure-cybersecurity-core.xlsx
- Industry Tools http://www.nist.gov/cyberframework/cybersecurity-framework-industry-resources.cfm

# Questions

Thank You

# Dan Ramey – Contact Information

Dan Ramey — CPA/CFF/ABV/CITP, CVA,

CIA/CRMA, CISA/CISM, CMA, CFE

Houston Financial Forensics, LLC

www.houstonfinancialforensics.com

Email: dan@houstonfinancialforensics.com

Cell: 832.567.8601

http://www.linkedin.com/in/danramey