



2017

RETIREMENT CONFERENCE

Cybersecurity Tips and Best Practices

A 2017 Update



Agenda

- Cybersecurity Risks in 2017
- The Impacts of a Data Breach
- Social Engineering and Phishing Scams
- Tips and Best Practices to Keep Yourself and Your Organization Safe



What the Experts Say

"Cyber espionage constitutes the greatest transfer of wealth in history."

Gen. Keith Alexander
NSA Director, 2012

"There are only two types of companies: those that have been hacked, and those that will be."

Robert Mueller
FBI Director, 2012



Cybersecurity Risks in 2017

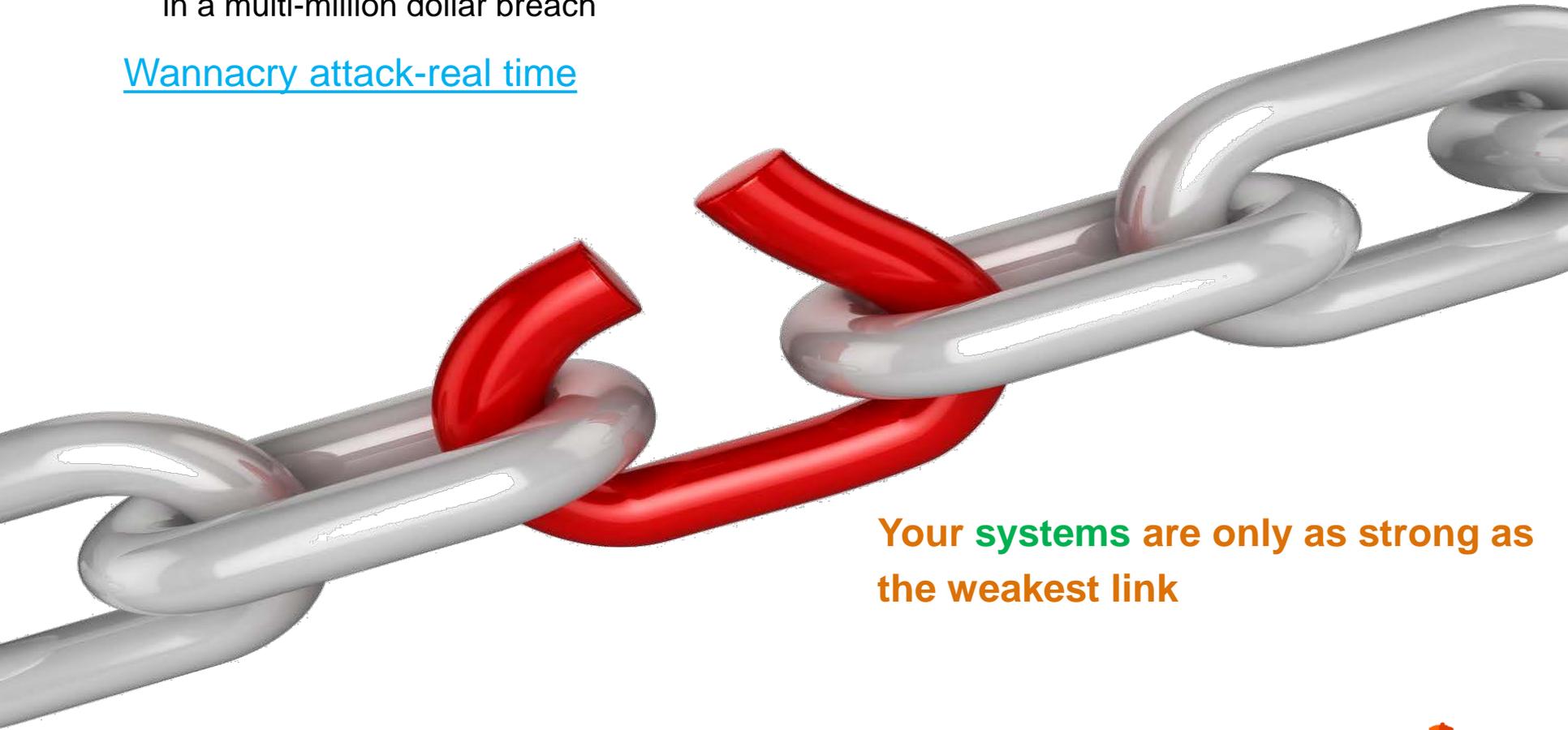


Persistent Imminent Risk

Hackers only need to be right once

- In some cases literally one wrong click is all it takes to launch a cyber attack that could result in a multi-million dollar breach

[Wannacry attack-real time](#)



Your systems are only as strong as the weakest link



Wannacry Ransomware Worldwide Attack

- [230K+ infections in over 150+ countries in 5 days](#)
- Malicious software can run in 27 languages
- Multiple attack vectors, including phishing
- Encrypted each file on victim's system with a random key
- Demanded bitcoin ransom equal to \$300 - \$600 per victim
- Spread itself to other systems connected to the victim (worm)
- Appeared to be targeting primarily telecommunications, hospitals, universities and transportation industries
 - Much more widespread impact
 - Dependent organizations may be subsequently impacted



2017 Ransomware Attacks

• WannaCry

- Leveraged leaked NSA hacking techniques and tools
- Can avoid antivirus scans
- Attack created by relative amateur hackers
- Later “Wannacry 2.0” attacks without the mistakes

• Subsequent “Ransomware” Attacks

- Cryptocurrency Miner – larger scale, no ransom notes
- Shadow Brokers “Data dump of the month” membership
 - Nuclear data, Windows 10 exploit data, etc.
- Petya and “Not-Petya” – considered cyberwarfare, not ransomware



University Pays Nearly \$16,000 in Ransomware Attack



Hacking Attack has Security Experts Scrambling to Contain Fallout

Leer en español

By MARK SCOTT MAY 13, 2017

Ransomware Attack Threats

- Fastest growing malware threat for all users on all types of computers
- Multiple types of ransomware spreading (e.g. Locky, ykcol, etc.)
- >4000 ransomware attacks daily since Jan 1, 2016
- 300% increase over 2015
- Typically delivered via phishing scams



Considerations Before Paying a Ransom

- **No Guarantee** - Paying a ransom does not guarantee an organization will regain access to their data
 - Some decryption keys have not been provided in the past
 - Some ransoms have been decoys for more nefarious activities
- **Repeated Attacks** - Some victims who paid the demand were targeted again by cyber criminals because they were willing to pay and/or had not remediated vulnerabilities
- **Increased Demands** - After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key
- **Supporting Cybercrime** - Paying encourages the ransomware criminal business model



18 Industry-Recommended Ransomware Mitigation Actions

- Cybersecurity awareness training programs
- Strong spam filters preventing phishing emails
- Authenticate inbound email to prevent spoofing
- Scan all incoming & outgoing email for threat detection and filtering executable files
- Configure firewalls to block access to known malicious IP addresses
- Patch operating systems, software and firmware on devices
 - **MERS performs monthly vulnerability scans**
- Conduct automatic regular anti-virus & anti-malware scans
- Manage the use of privileged accounts to least privilege needed and use grant/revoke controls
- Disable macro scripts by default



18 Industry-Recommended Ransomware Mitigation Actions

- Configure access controls (read/write capabilities etc.)
- Implement Software Restriction Policies to prevent programs from executing from common ransomware locations
- **Disable Remote Desktop protocols**
- **Use Application Whitelisting to only allow systems to execute known secure programs**
- Execute operating systems and programs in a virtual environment
- **Segment networks physically & logically**
- Backup data and test backups regularly
- **Conduct annual penetration tests**
- Secure backups and store backups offline



The Impacts of a Data Breach



Equifax Data Breach - Chronology

- Mar 2017 - Smaller breach discovered
 - TALX payroll service portal breach
 - Hackers “guessed” registered users personal questions
 - Reset PIN numbers & obtained users W-2 forms
 - Happened between Apr 17, 2016 – Mar 29, 2017
- May-Jul 29, 2017 - 143M U.S. consumer records exposed
 - Names, birth dates, SSN, addresses, driver’s licenses, etc.
 - 209K credit card numbers
 - Known vulnerability in Apache/Struts web software environment
 - Breach unchecked for 77 days
- Aug 2017 – Key Equifax execs sell \$1.8M of stock
- Sep 7, 2017 – Equifax announces breach
- Sep 18, 2017 – CIO & CSO “retire” immediately



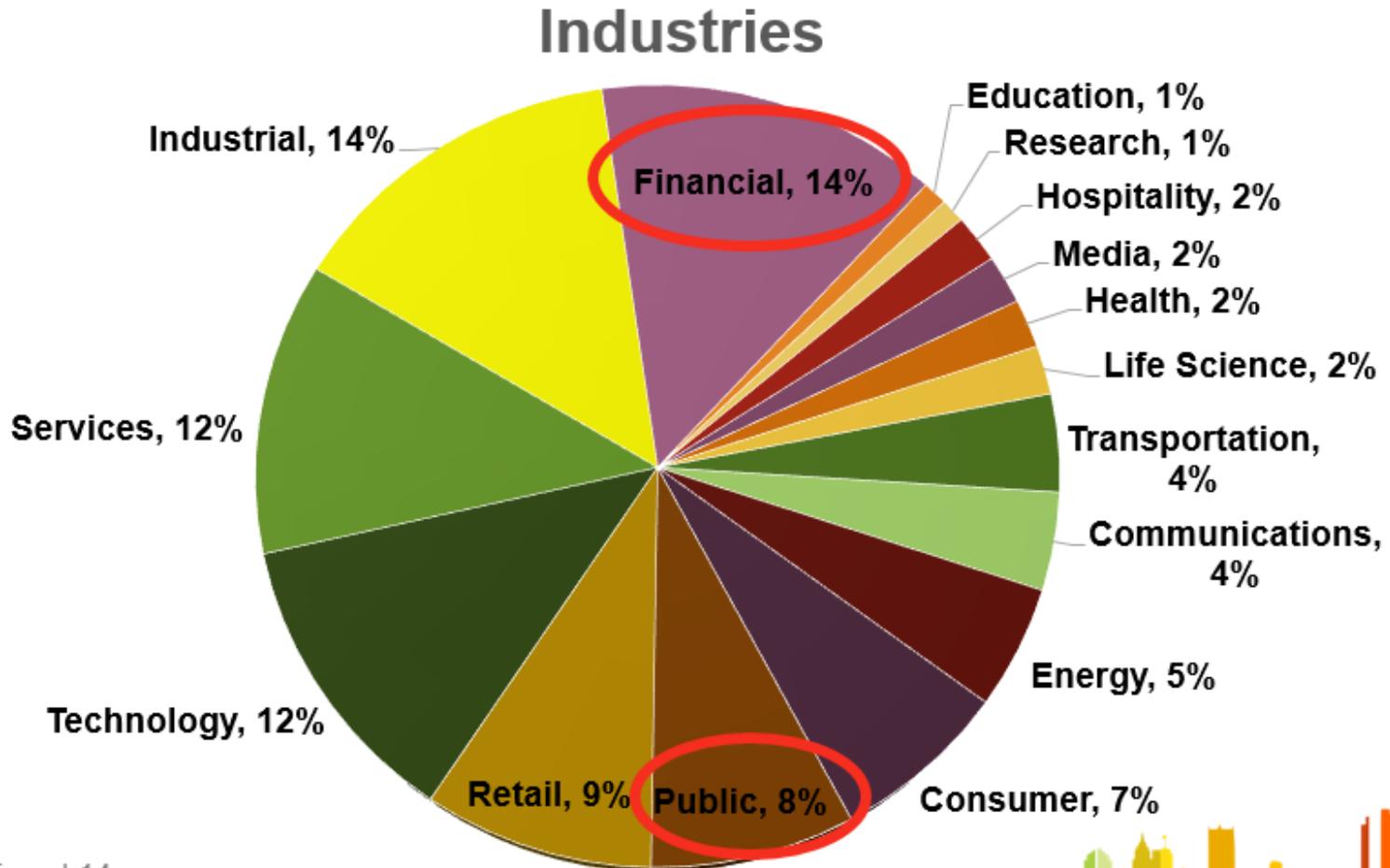
Equifax Data Breach Impacts

- Severely shaken consumer confidence in Equifax and online financial options in general
- Loss of credibility, integrity & sincerity
 - Equifax attempting to leverage crisis to sell their own credit card monitoring services
 - Attempting to get customers to waive their class action lawsuit rights if they sign up for any credit monitoring service offered
 - Multiple formal investigations, including FTC and SEC investigations into sale of stock by executives
- May just be a prelude to larger banking system attack
- Keep close watch on your credit card & banking statements and credit reports for fraud activity
- Change passwords, security questions, etc. if you think you may be at risk
- Beware of increased and more advanced phishing attempts
 - *E.g. 'To show this is not a phishing email, we have included the month of your birth and the last 3 digits of your phone number'*



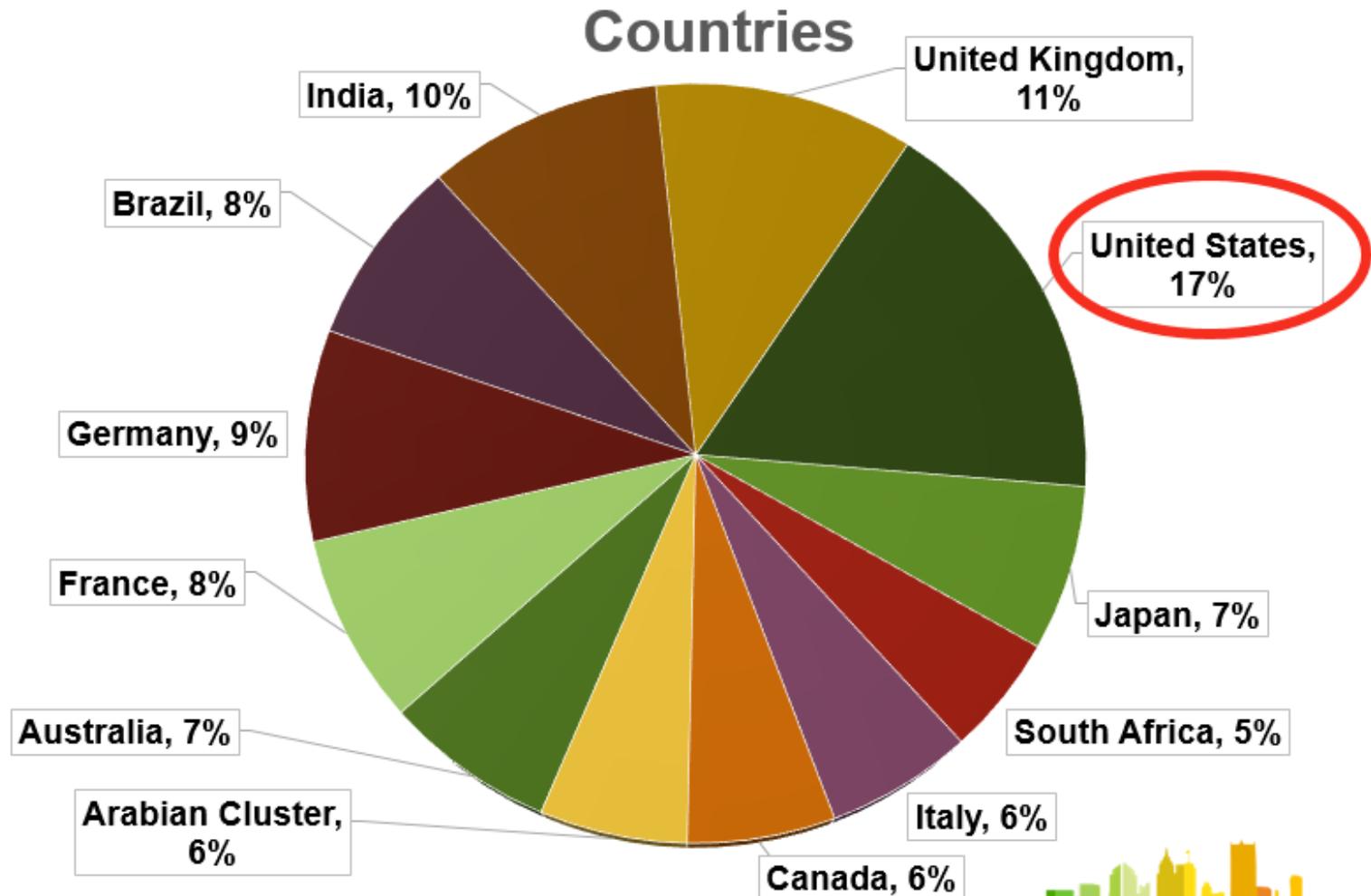
Data Breach Impacts, cont'd.

The 2016 **Cost of Data Breach Study** covered 383 companies in 16 industries and 12 countries



Data Breach Impacts, cont'd.

The 2016 **Cost of Data Breach Study** covered 383 companies in 16 industries and 12 countries



Data Breach Impacts, cont'd.



The Cost of a Data Breach

A breach of just 1,000 records with Personally Identifiable Information (PII) could cost \$1M

(Not including any ransom or extortion that may be paid)

Examples:

- One database table
- Large spreadsheet
- One payroll report

Direct Damages

- Professional services (investigation and remediation, etc.)
- Lost business opportunities (disclosure, public reputation, etc.)
- Down-time

Indirect Damages

- Staffing increases and changes
- Increased employee training
- System repair and improvements
- Increased insurance costs



The Cost of a Data Breach

The Cost of Data Breach

Data breach hits organizations squarely in the wallet. The average cost per record goes up depending on who or what caused the exposure.



Source: Ponemon Institute 2015, Cost of Data Breach Study: Global Analysis



Code42 is a SaaS provider of enterprise endpoint data protection and security. We offer highly secure cloud backup to support recovery from data loss, compliance with data privacy regulations, and higher order data tools including eDiscovery and data movement analytics. www.code42.com.



Humans are Vulnerable

The Role of Human Error in Successful Security Attacks

September 2, 2014 | By [Fran Howarth](#)



All humans make mistakes. One of the most intriguing findings from IBM's "2014 Cyber Security Intelligence

Index" is that **95 percent of all security incidents involve human error**. Many of these are successful

who prey on human weakness in order to lure insiders within organizations to unwittingly provide them with access to sensitive information.

These mistakes are costly since they



Social Engineering and Phishing Scams



Cybersecurity Realities Today

Social Engineering Epidemic

Hacker Industry Premise (Trojan Horse)

If the fortress is impenetrable, trick someone into opening a door



Survival of the Fittest

Cybersecurity Industry Premise

Make it so difficult for hackers that they attack other targets, while not making it more difficult for business users or customers



Social Engineering and Phishing Scams

Trickery or deception for the purpose of information gathering, fraud, or computer system access



In most cases the attacker never comes face-to-face with the victim



Common Social Engineering Methods

- **Public Wi-Fi and Hotel Wi-Fi**
- **Tailgating**
 - Access a secure building or secure area
- **Baiting**
 - Purposely leaving media such as a flash drive to be picked up and plugged in to a computer
- **Phishing (Trick-to-click)**
 - [Vishing \(Voice phishing\)](#)
 - Spear Phishing (Targeted phishing)
 - Whaling (Phishing targeting executives)



Types of Phishing



Spear Phishing

- Phishing attempts can be directed at specific individuals or companies
- Personal information about the target is used to increase the probability of success
- This technique, by far the most successful on the internet today, ***accounts for 91% of attacks***



Types of Phishing, cont'd.

Whaling

- Whaling is an attack directed specifically at senior executives and other high-profile targets within businesses
- A whaling attack email is often written as a legal subpoena, customer complaint, or executive issue



Phishing Lures

Screenshot of Phishing Email


Dear CitiBank customer,
of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

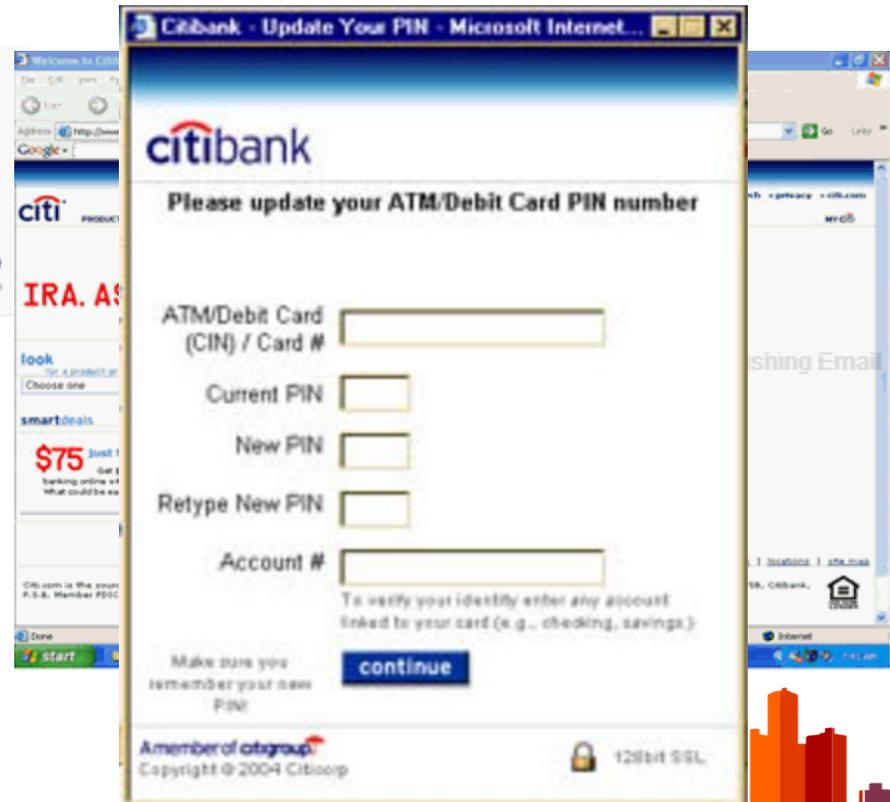
This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

https://web.da-us.citibank.com/signin/scripts/login/user_setup.jsp
Thank you for your prompt attention to this matter and thank you for using CitiBank!
Citi® Identity Theft Solutions
Do not reply to this email as it is an unmonitored alias
A member of citigroup
Copyright © 2004 Citicorp

The more applicable or urgent the scenario, the greater risk of falling prey to phishing

- FBI, legal threats for non-reply
- UPS message at Christmas
- Resend W-2 forms at tax time, etc.

These email and website examples are relatively easy to distinguish



Phishing Lures Targeting Retirees

Subject: URGENT REPLY NEEDED!
From: prof.ccsoludo101@bank.cboa.com
Date: 5/29/2008 9:15 AM
To: [no To-header on input <unlisted-recipients>](#)

False urgency defined to get you act without thinking

CENTRAL BANK OF NIGERIA
TINUBU SQUARE, VICTORIA ISLAND
LAGOS-NIGERIA
Foreign Remittance Diplomatic Department
Email: prof.ccsoludo101@bank.cboa.com

If it sounds too good to be true it usually is.

Dear Friend,

Generic greeting

Obvious grammar or spelling errors

I know that this message will come to you as a surprise. I am the Bill and Exchange Manager in Central Bank of Nigeria (CBOA). I hoped that you will not expose or betray this trust and confident that I am about to repose on you for the mutual benefit of our families.

I need your urgent assistance in transferring the sum of (USD \$20M) to your account within 10 to 14 banking days. This money has been dormant for years in our bank without claim. I want the bank to release the money to you as the nearest person to our deceased customer (the owner of the account) died along with his supposed next of kin in an air crash since July 2001.

I don't want the money to go into our bank treasurer account as an abandoned fund. So this is the reason why I contacted you so that the bank can release the money to you as the next of kin to the deceased customer. Please I would like you to keep this proposal as a top secret and delete it if you are not interested.

Upon receipt of your reply, I will give you full details on how the business will be executed and also note that you will have 40% of the above mentioned sum if you agree to handle this business with me? And 10% will be set aside for any expenses that warrant on the process before the fund get into your account such as telephone calls bills (etc).

Please reply to me at prof.ccsoludo101@bank.cboa.com

Hover over it

The email link is really a web link

Yours Faithfully,

Prof. Charles C. Soludo (CBOA Governor)
Email: prof.ccsoludo101@bank.cboa.com

The status bar reveals the real web address.

Never click on an untrusted link

Go directly to the link referenced to be safe

<http://cybertangent.com/UFL.edu>

Statistics

- Sweepstakes and lottery scams alone trick Americans out of **billions** of dollars every year
- An estimated 10%–15% of the U.S. population fall victim each year
- Average age is 55–65 years old
- Scams under-reported
 - Most too ashamed to report being victimized
 - More than 90% of lottery scams not reported

(Source: AARP)



Tips and Best Practices to Keep Yourself and Your Organization Safe



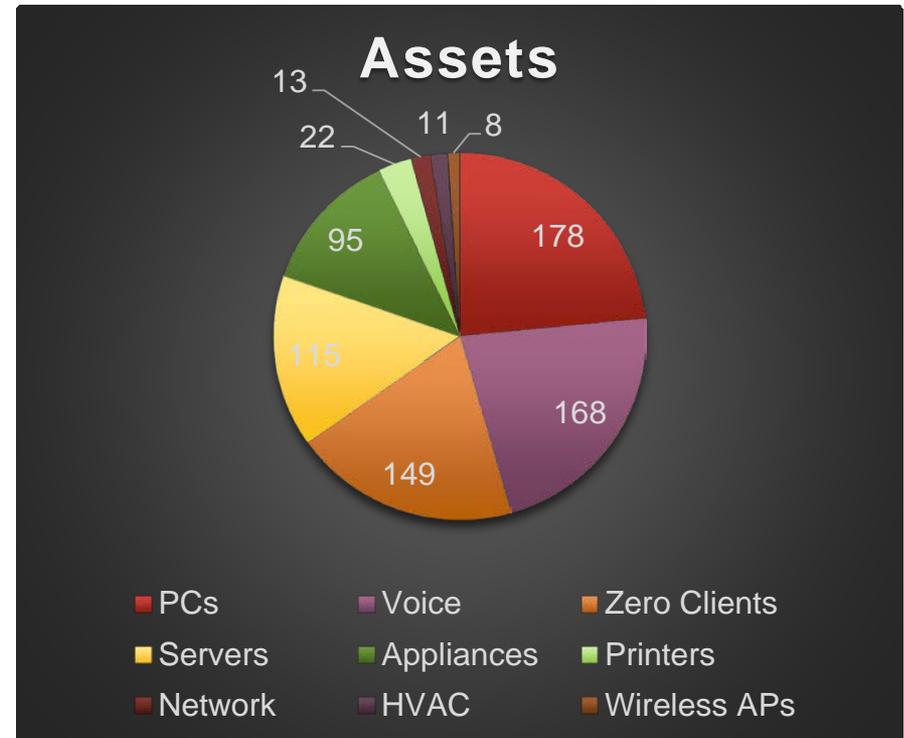
Tips to Securely Communicate & Transact Business with MERS:

- Don't reply directly to e-newsletters, event notifications or any other type of mass email. Contact the MERS Service Center if you have any questions about the information you receive
- Use your secure myMERS account to transact MERS business such as changing your investment allocations and updating your contact information
- **If you must send MERS sensitive documents via email, contact the Service Center first to have an encrypted email sent to you from MERS, to reply with your sensitive document attachments**
- Use the tips we just learned to ensure that all emails that appear to be coming from a MERS address (ex:jdoe@**mersofmich.com**) aren't phishing scams
- Report any suspicious emails or other forms of communication that appear to be coming from MERS to the Service Center



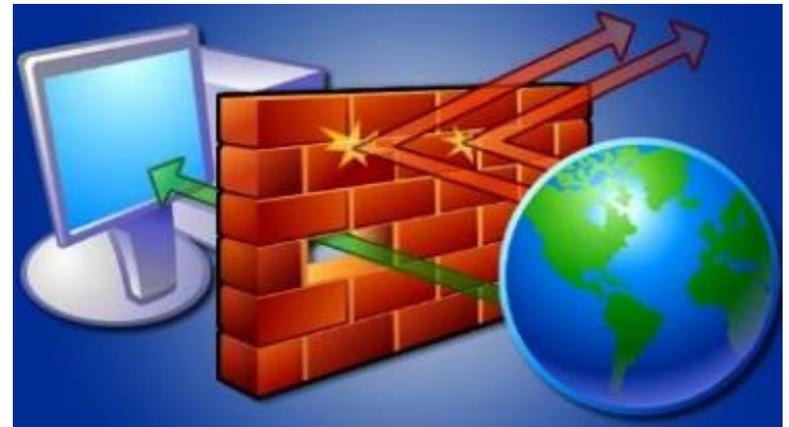
IT Support/Vulnerability Scope

- **Many devices to secure**
 - E.g. MERS has 130 employees but 800+ devices
 - Includes very few smartphones (BYOD)
- **Vulnerabilities are classified by severity:**
 - Moderate (information gathering)
 - Severe (disruptive, basic access, etc.)
 - Critical (full access, privilege escalation, known exploits, etc.)
- **Implement tools & process to identify & remediate vulnerabilities**



MERS Progress Since 2016 Annual Conference

- Updated monthly online security awareness training for all employees and on-site long-term contractors
- Updated MERS-wide internal phishing testing
- Network segmentation started
- Successful penetration test
- Cybersecurity insurance
- Vendor security screening
- Monthly vulnerability testing & remediation
- Additional cybersecurity association memberships
 - Financial Services Information Sharing and Analysis Center (FS-ISAC)



Incident Management

- Isolate infected computers
- Isolate or power-off partially infected computers
- Immediately take backup systems offline to keep them secure
- Contact cyber-insurance resources
 - Contact law enforcement immediately (FBI)
- Collect & secure partial portions of ransomed data that might exist
- Change all online account passwords & network passwords after removing the system from the network
- Delete Registry values and files to stop the program from loading
- Implement cybersecurity incident response and business continuity plans



Personal Cybersecurity Tips

- **Maintain complex passwords**

- Today non-complex passwords can be broken in hours
- Leads directly to your wallet and the bottom line
- Never share your password or write it down anywhere
- Never use the same password on multiple sites
 - 75GB database with 560M passwords exposed, including passwords from LinkedIn, Dropbox, Neopets, RiverCityMedia, Tumblr, MySpace and Lastfm, to name a few.



- **Use 2-Factor Authentication when possible**

- Requires at least 2 pieces of information to authenticate
 - Typically something you know, something you have, or something you are (biometrics)
- Prevents someone from being able to login as you from anywhere else
- **Setup automatic patch updates on personal computers & keep smartphones updated**

- **Beware of the phisherman**

- If it looks too good to be true – it probably is
- If it sounds too urgent – it probably is not
- If it sounds too demanding – it probably is not

- **[Don't overshare on social media](#)**

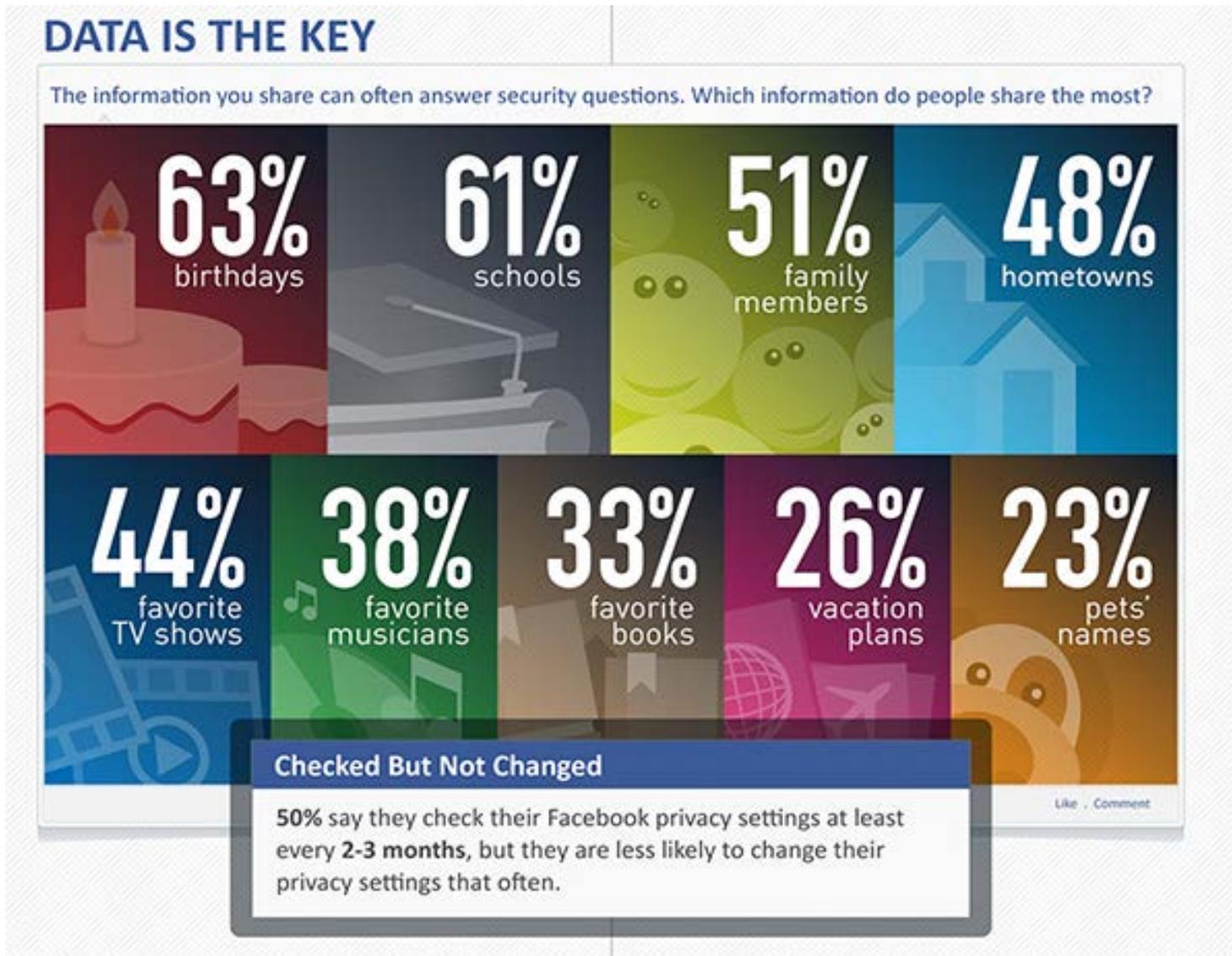


Social Media Dangers

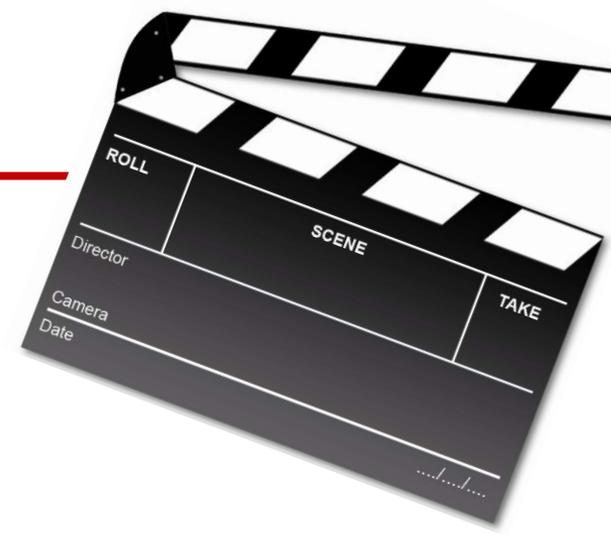
- “TMI” – People are oversharing personal and company information, which can be dangerous - it’s like handing ammunition to an attacker
- Targeted phishing attacks (“spear phishing”) can be built against you or your family, employees, colleagues or friends based on this type of information



Social Media Dangers



Key Action Items



- **Remain Vigilant**
 - Watch for tell-tale signs of malicious content report them
 - Cybersecurity vigilance is never-ending
- **Security awareness / phishing**
 - Acquire and stay up-to-date on security awareness training
 - E.g. Security Mentor, KnowBe4, etc.
 - Allow staff to show security awareness trainings to their family members
- **Protect Yourself (and thereby your family & organization too!)**
 - Keep personal technology patched and up-to-date – including smartphones
 - Monitor your family members' online hygiene, especially teens & “tweens”
 - Protecting your identity & technology protects your financial security and everyone connected to you in any way

MERS is committed to keeping your data safe!



Cybersecurity Information Questions



MERS of Michigan



MUNICIPAL EMPLOYEES' RETIREMENT SYSTEM

1134 Municipal Way

Lansing, MI 48917

800.767.MERS (6377)

www.mersofmich.com

This presentation contains a summary description of MERS benefits, policies or procedures. MERS has made every effort to ensure that the information provided is accurate and up to date. Where the publication conflicts with the relevant Plan Document, the Plan Document controls.

