What The Hack!

Aldo Leiva

Jorge Rey

LUBELL | ROSEN

KAUFMAN | ROSSIN

Agenda

- Introduction
- Cybersecurity Trends
- Legal Framework For Cybersecurity Compliance
- How Are Organizations Getting Hacked
- Oops, you clicked on the link. Now what?
- Best Practices and Discussion

Disclosure

- These materials should not be considered legal advice and are not intended to nor do they create an attorney-client relationship
- The materials are general and may not apply to a particular individual legal or factual circumstances
- Information presented is based on educational needs of attendees and independent of commercial interests.

Cybersecurity Trends

Advanced Threat Innovation

Detection & Response Threshold

3rd Party Exploits

Stuxnet

Document Malware

Conficker

Worms

APT

OS Exploits

Cyber Crime

DoD Intrusions

Virus

Morris

Technology & Complexity

Cloud / Mobile

Virtualization

VoIP

Desktops

Mainframes

Typewriters

Phones

Paper

>1940

Ameriprise

Heartland

Target

Today

AOL

TJ Maxx

Countrywide

Sony

RSA

JPMC

DNC / NFL

LUBELL | ROSEN

Legal Framework for Cybersecurity

- Federal Law
- Guidelines (IRS, NY State Dept Financial Services, AICPA Code of Conduct)
- State Law
- Contract Law

Federal Law

- More than 30 Federal laws relate to Data Protection or Privacy Protections
- *Electronic Communications Privacy Act of 1986 (ECPA)* prohibits unauthorized electronic eavesdropping.
- *Cyber Security Research and Development Act* (2002) established research responsibilities in cybersecurity for the National Science Foundation (NSF) and NIST.

Federal Law

- *Gramm Leach Bliley Act*- Requires financial institutions to protect the security and confidentiality of customers' personal information; authorized regulations for that purpose.
- *Fair and Accurate Credit Transactions Act of 2003* (FACTA)- Required the FTC and other agencies to develop guidelines for identity theft prevention programs in financial institutions, including "red flags" indicating possible identity theft.
- Health Insurance Portability and Accountability Act (HIPAA)

IRS Guidelines/Resources

- IRS Publication 4557- Safeguarding Taxpayer Data
  - Security Software
  - Policies and Procedures/Education
  - Scanning/Updates
  - Data Loss Prevention
- IRS Publication 4524- Taxes, Security
  - Security measures for clients/taxpayers

IRS Alerts

- Irs.gov
    - Security Summit Homepage
- IRS Twitter/Facebook

New York State Department of Financial Services (DFS)

- 2014
- Cybersecurity protocol for banks- but good benchmark for professional firms to start process of data protection

AICPA Code of Professional Conduct

- Rule 301- CPAs shall not disclose any confidential client information without the specific consent of the client
- Includes loss of information to unauthorized parties by malware, inadvertent disclosure, hacking, or other means.
- Applies to all CPA practice areas, including tax, audit, advisory and other services
- Data sets retained by CPA

Florida Information Protection Act

- Effective July 1, 2014
- Applies to “a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information.”
- Includes accountants, lawyers, tax preparation services

FIPA – Personal Information

- Individual's first name or first initial in combination with any one or more of the following:

(1) SSN

(2) Driver License or ID card number

(3) Financial Account number/credit card number

(4) Medical History, Treatment, Diagnosis

(5) Health insurance policy/ID number

OR

FIPA – Personal Information

- User name or email address in combination with password or security question and answer that would permit access to an online account

Exceptions

- Does not include information about an individual that has been made publicly available by a federal, state, or local government entity
- Does not include information that is encrypted, secured, or modified by any method/technology that removes elements that personally identify an individual or renders it unusable

PII stored by Tax Professionals

- Employee Information (SSN, DOB)
- Financial Information (tax returns)
- Payment information
- Documentary support (bank info, checks, etc.)

FIPA Requirement for Data Security

- Each covered entity SHALL take reasonable measures to protect and secure data in electronic form containing personal information
- “Reasonable measures” are not defined in the statute

Breach Notice Requirements

- Notice to affected individuals within 30 days from the time breach is discovered
- Must notify each individual “in this state” whose personal information was or is believed to have been accessed as a result of a breach
- Such notice may be delayed upon written request of law enforcement authorities, if notice would interfere with a criminal investigation

Notice Requirements (500+)

- If breach affects 500 or more persons, must also notify Florida Department of Legal Affairs no later than 30 days after determination of the breach or reason to believe a breach occurred, although an additional period of up to 15 days may be granted for good cause, if so authorized by the Florida Department of Legal Affairs

Notice Requirements (1,000+)

- If the breach requires notification to more than 1,000 individuals at a single time, the covered entity must also notify credit reporting agencies “without unreasonable delay”

Notice Exemptions

- No notice required IF after appropriate investigation and consultation with the relevant law enforcement authorities, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or financial harm to affected individuals
- Determination must be documented and filed with FL Department of Legal Affairs within 30 days

Notification of breach by vendor

- Third parties must notify you of a breach no more than 10 days after a data breach
- Once notified, affected parties must be notified within 30 days of such notice

FIPA Penalties

- (1) $ 1,000 per day, during the first 30 days
- (2) $ 50,000 for each following 30 day period (up to 180 days)
- (3) Up to a maximum of $ 500,000.00 for any violation

Out of State Implications

- Tax professionals may be storing PII of individuals that have moved and now reside in other states
- If such server containing such PII is breached, other state law data breach notification laws may apply (47 different laws- no national standard)

Other Considerations

- HIPAA/HITECH
- PICC
- EU Data Protection Laws, other foreign data protection laws

Other Liability

- Contractual- Law firm/hiring entity- indemnification
- Spoliation claim (litigation)
- Reputation
- Identity Theft – Negligence

How Are Organizations Getting Hacked

Phishing and Spear phishing is the top cyber threat to you and your organization.

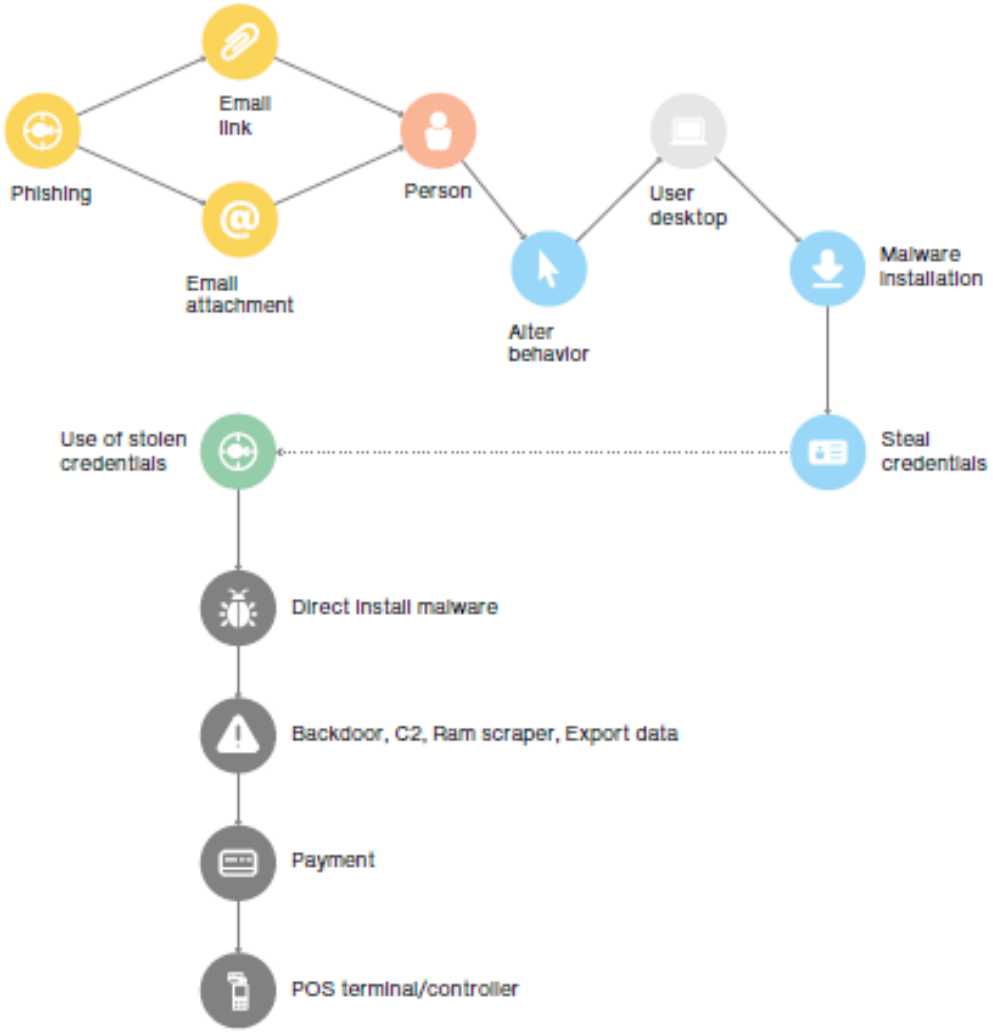
- Every day 80,000 people fall victim to a phishing scam
- Around 156 million phishing emails are send every day.
- 4,000 ransomware attacks have occurred daily (since 2016)
- On average, 12% of people get phished (click, download, etc…), but only 3% report it to management.

Some of the Attacks

For Profit	Wire Fraud	State Attacks on Business	State Attacks on Government
• JPMorgan Chase • eBay • Target • Ransomware Attacks • Yahoo	• Ubiquiti Networks	• Anthem • Sony Pictures • Entertainment • ThyssenKrupp	• Office of Personnel Management • US Government

Democratic National Committee

How It Happens



Fraud Sample

From: Elizabeth Rockowitz
Sent: Monday, December 19, 2016 4:04 PM
To: Jorge Rey
Subject: Request

Jorge,

Are you busy?Let me know.

Regards
Elizabeth

-----Original Message-----
From: Jorge Rey <JRey@KAUFMANROSSIN.COM>
To: 'Elizabeth Rockowitz'
Sent: Mon, Dec 19, 2016 1:23 pm
Subject: RE: Request

No, why what's up?

Jorge Rey, CISA
Director

Fraud Sample

From: Elizabeth Rockowitz'
Sent: Monday, December 19, 2016 4:27 PM
To: Jorge Rey
Subject: RE: Request

Jorge,

I need you to transfer a payment today, Get back to me if you are available so i can forward you the beneficiary details.

Regards
Elizabeth

From: Elizabeth Rockowitz' [mailto:john_morrow3@aol.com]
Sent: Monday, December 19, 2016 4:33 PM
To: Jorge Rey
Subject: Re: Request

It is imperative the payment goes out today. Below beneficiary information. I would appreciate if this could be paid today if possible for the applicable fee so they can get it today.

Account Name: Laurie Janell wells
Bank Name: Bank of America
Bank Address: 59/littleyork center Houston TX 7093 US
Type Of Accountt: Checking
Account Number: 488065983519
Routing Number: 111000025
Amount: $1450.00

Kindly send me an email with the payment receipt once completed.

Regards
Elizabeth

Oops, you clicked on the link. Now what?

- Prepare for Assessment
- Retain forensic specialist and counsel to trigger attorney client privilege
- Consider law enforcement notification
- Follow breach assessment/response plan
- Preserve Evidence/Lock down system
- Assess breach notification requirements

Oops, you clicked on the link. What else?

- Notify affected parties
- Notify relevant state/federal authorities
- Public Information Officer and/or external media consultant
- Notify credit card companies and credit reporting bureaus

Best Practices & Discussion

- Assess your infrastructure (preferably by independent third party) to ensure that "reasonable measures" are in place
- Third party audit to ensure that PII is encrypted according to applicable law
- Tech inventory
- Assess existing policies and procedures
- Assess exposure and cyberliability coverage

Be Proactive

- Written response plans, policies and procedures
- Confidentiality agreements
- Education/training
- System assessments
- Indemnification from subcontractors/vendors
- Consult with Counsel and Data Security Experts

Thank You

Jorge Rey
jrey@kaufmanrossin.com
(561) 620-1727

Aldo Leiva
aml@lubellrosen.com
(305) 442-9211