Employee Privacy in the Electronic Workplace

Jane Shea and Michael Severini

Today's Speakers

- Jane Hils Shea, Esq.
  Member & Chair of Data Privacy and Information Security Practice Group
  Frost Brown Todd LLC
  jshea@fbtlaw.com
- Michael Severini, CISSP, CISM
  Information Security & Compliance Manager
  Frost Brown Todd LLC
  mseverini@fbtlaw.com

Privacy vs. Security

You must implement security

to ensure privacy

Agenda

1. HR Data Collection and Technological Employee Monitoring
2. Employee expectations of privacy and HR Policies
3. Information Security Tools
4. Current Cyber Threats
5. Best Practices for Data Security in the HR Space

Difference between Privacy and Security

- **Security** is a process….**privacy** is a consequence
- **Security** is the strategy…..**privacy** is the outcome
- **Security** is action ….**privacy** is the result of successful action

- The concepts are inextricably related, and company organization should enable and encourage that relationship

Hypothetical Fact Pattern

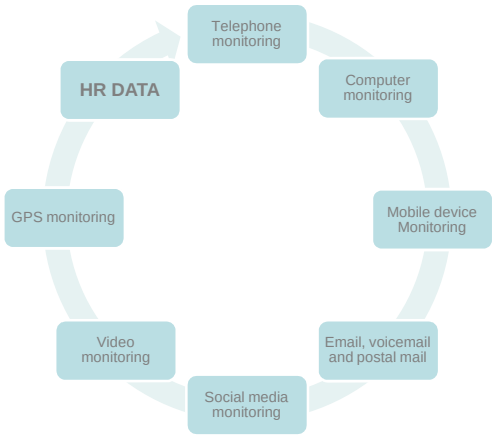
- Employee mole trying to siphon off company clients
  - Search of cubicle, laptop, cell phone
  - What is permissible?

U.S. Privacy Protections

- The U. S. Constitution contains no express right to privacy
- Since 1923, the Supreme Court has broadly read the "liberty" guarantee of the Fourteenth Amendment to guarantee a fairly broad right of privacy of the Constitution.
- Federal, state and local laws provide basic source of protection against invasion of privacy by private parties
- Tort of intrusion upon seclusion

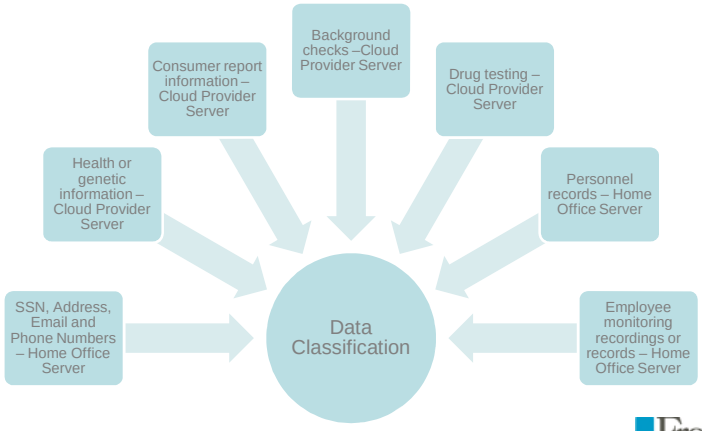
Frost Brown Todd LLC ATTORNEYS

What Are the Employee's Expectations of Privacy in a Technical Workplace?



Frost Brown Todd LLC ATTORNEYS

Data Mapping - Types of HR Data at Risk



Employer HR Policies

- Managed by Published Company Policies
  - Post-hiring Drug and Alcohol Testing
  - Monitoring Practices
  - Searches
  - BYOD
  - Record Retention

Risks in Failing to Protect Data

- Data Breach Notifications
- Lawsuits
- Reputational Risk

2016 Cybersecurity Threats

- **Phishing Email Scams**
  - **Social Engineering** - The single biggest security threat of 2016 will be people.
  - **Ransomware** will become even more prevalent.
  - **CEO Fraud** aka Business Email Compromise.

What is Phishing Anyway?

Phishing is any attempt to try and acquire sensitive information or steal money from you or your company.

- Email
  - The most common form of phishing is by email.
- Phone
  - Someone contacts you unexpectedly and asks for your personal information such as your financial institution account number, or Social Security number.
- Text Message
  - **SMShising** – Text messaging purporting to be from a financial institution saying that account has been suspended.

Frost Brown Todd LLC ATTORNEYS

Phishing used to be easy to spot

Frost Brown Todd LLC ATTORNEYS

Simple Phishing Example

Email address not from your company

From: Outlookhelpdesk@micro.com
Sent: Tuesday, February 20, 2016 9:11 AM
Subject: Microsoft Outlook Verification

dear outlook user, IT Helpdesk requires your immediate re-activation of your Email account. This is to upgrade email account to new version of Microsoft Outlook. Inability to complete this procedure will render your account inactivate. CLICK HERE to activate.

IT Helpdesk

Generic content, incorrect spelling, poor grammar

Frost Brown Todd LLC ATTORNEYS

Complex Phishing Example

Real client email

From: North Financial [mailto:john.snow@northfinance.com]
Sent: Tuesday, February 16, 2016 9:37 AM
Subject: Your Quicken Bill Pay Invoice from 02/12/2016.

Realistic content

Greetings from Quicken Billpay-center!

Thank you for your business, and we look forward to the opportunity of serving you again in the future.

Click the link below to view your Invoice.

http://www.billpay-center.com/invoices/007448322.doc

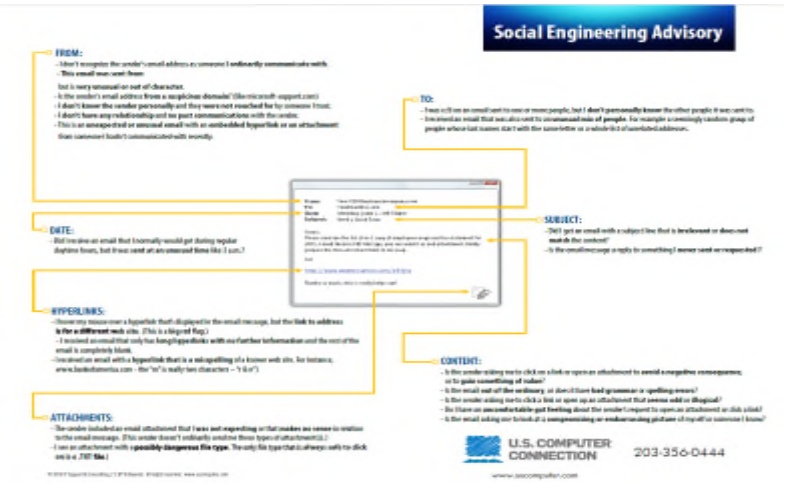
If you have any questions call us at 1-877-488-8843.

Sincerely,
Billpay-center

This message has been scanned for viruses and dangerous content by MailScanner, and is believed to be clean.

Frost Brown Todd LLC ATTORNEYS

Phishing Overview



Frost Brown Todd LLC ATTORNEYS

Social Engineering

- Art of manipulating people.
- Weakest security link is people.
- Social Engineering is easier to exploit.

Frost Brown Todd LLC ATTORNEYS

Social Engineering

Ransomware

- **Ransomware** is an especially aggressive form of malware that holds your computer, data or a particular function “hostage” by encrypting all of the files on your computer until a ransom is paid to the creator of the malware. Attackers commonly use email as the delivery method in the form of infected Word attachments.

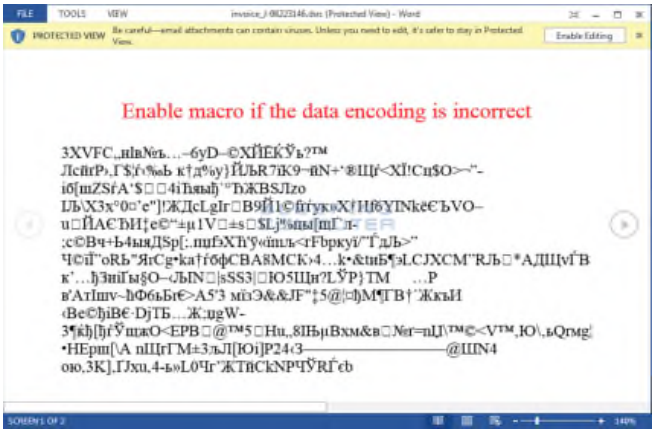
Ransomware

Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files

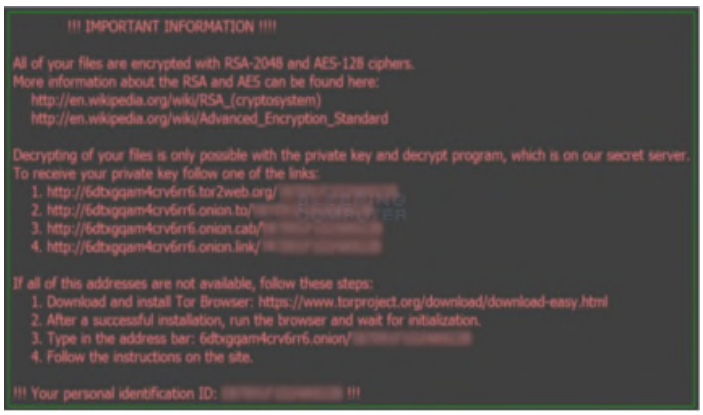
Frost Brown Todd LLC ATTORNEYS

Ransomware Example



Frost Brown Todd LLC ATTORNEYS

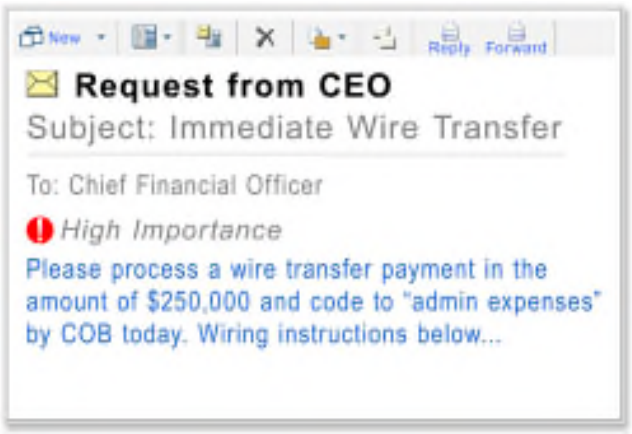
Ransomware Example



CEO Fraud aka Business Email Compromise

- Look and feel of legitimate email from your CEO.
- “Urgent” email from CEO requesting wire transfer.
- Targets HR and Finance departments
- The requested payment method is wire – usually internationally.

CEO Fraud aka Business Email Compromise



Frost Brown Todd LLC ATTORNEYS

CEO Fraud aka Business Email Compromise

Technology | CyberSecurity

Hackers carry out $55m cyber heist from Boeing aerospace parts manufacturer

By James Billington
January 27, 2016 20:25 GMT

Hackers hit an aerospace manufacturer in a $55 million spear phishing heist (Getty)

An aerospace manufacturer that supplies engine and interior parts for the likes of Airbus and Boeing has been hit by a massive cyber attack that has seen hackers take off with $55m (€50m, £38m) from the company's accounts.

FACC, an Austrian company that has been a supplier to Airbus since 1989, revealed on its company blog that on 19 January the finance department "was the target of cyber fraud and became victim of fraudulent activities involving communication and information technologies".

Frost Brown Todd LLC ATTORNEYS

Don't be a CEO Fraud Mail Victim

- Beware of any urgent wire payment emails requests that call for secrecy and ask you to act quickly
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign- off by company personnel
- Carefully scrutinize all e-mail requests for transfer of funds to determine if the requests are out of the ordinary.

Can you spot the phish?

- Insert phishing email example (FBT marketing prizes for audience correct answers?

Can you spot the phish?

- Insert phishing email example (FBT marketing prizes for audience correct answers?

The Threat is Real!

Phishing

- Stats
- Stats
- Stats

Social Engineering

- Stats
- Stats
- Stats

Ransomware

- Ransomware doubled in 2015 and is expected to double again in 2016.
- Stats
- Stats

CEO aka Business Email Compromise

- 270% increase in identified victims since Jan 2015
- Exposed dollar loss from Oct 2013 – Oct 2015 **$798,897,959.25**
- Stats

WISP Components & Best Practices

- Know where the data resides
  - Data Mapping
- Include and highlight the Company Policies, including an Information Security Policy
- Create a culture of privacy
  - Regularly train employees on privacy and information security
- Include an Incident Response Plan
- Continually assess status of physical and technological security protections
- Protocols for secure disposal of sensitive personnel information

Frost Brown Todd LLC ATTORNEYS

Privacy Considerations for Data Subsets

- Federal and state law dictate permissible and impermissible uses and record retention periods for each of the various data subsets
- Certain industries and job types have additional limitations on uses and data collection

Frost Brown Todd LLC ATTORNEYS

Best Practices

- Designate Chief Information Security Officer
  - Not the IT Manager
- CISO should work regularly with Privacy Officer
- Get a Seat at the Information Security Team Table
- Advocate for and Familiarize yourself with Company WISP
- Train employees in policies and risks
- Advocate privacy by design

Frost Brown Todd LLC ATTORNEYS

- Questions and Comments?

- jshea@fbtlaw.com
- mseverini@fbtlaw.com

Frost Brown Todd LLC ATTORNEYS