



Employee Privacy in the Electronic Workplace

Jane Shea and Michael Severini

Today's Speakers

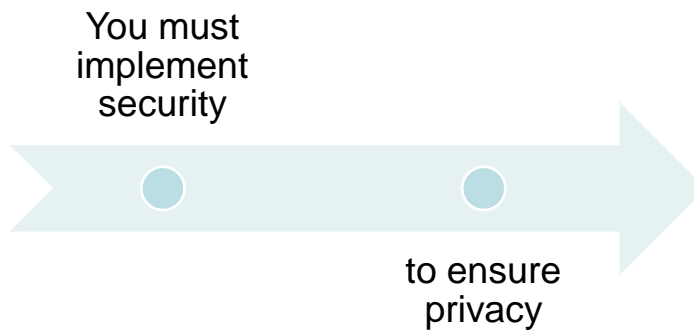
- Jane Hills Shea, Esq.
Member & Chair of Data
Privacy and Information
Security Practice Group
Frost Brown Todd LLC
- Michael Severini, CISSP,
CISM
Information Security &
Compliance Manager
Frost Brown Todd LLC

jshea@fbtlaw.com

mseverini@fbtlaw.com



Privacy vs. Security



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?



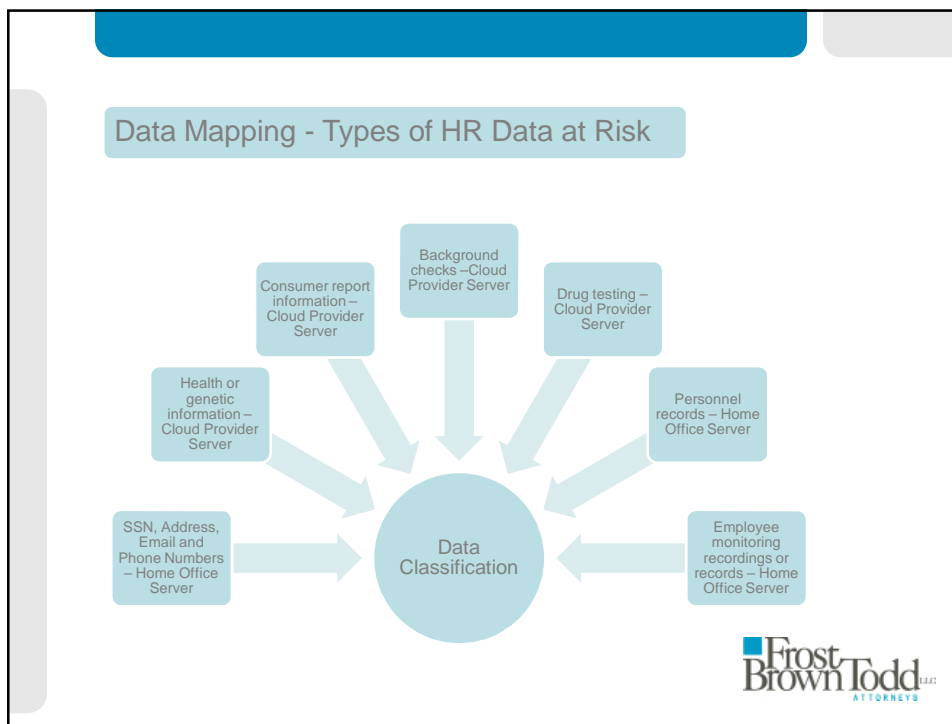
U.S. Privacy Protections

- 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



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





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.



Phishing used to be easy to spot



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



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.



Phishing Overview

Social Engineering Advisory

FROM:

- Don't recognize the sender's email address as someone I ordinarily communicate with.
- This email may come from:
 - but is very unusual or out of character.
 - the sender's email address from a suspicious domain (illegalsupport@support.com)
 - I don't know the sender personally and they were not reached for by someone I trust.
 - I don't have any relationship and no past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I don't communicate with usually.

TO:

- I see a list of email addresses or more people, but I don't personally know the other people it says, so it's a broadcast email that was also sent to someone else of people. For example, a company-wide group of people whose last names start with the same letter or a whole list of unrelated addresses.

DATE:

- Did I see an email that I normally would get during regular daytime hours, but it was sent at an unusual time like 3 am?

SUBJECT:

- Don't get an email with a subject line that is broken or doesn't match the content?
- Is the email message in reply to something I never sent or requested?

HYPERLINKS:

- There are misspelled hyperlinks that display for the email message, but the link is address to the different web site. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information and the end of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofamerica.com - the "a" is really two characters - "a a")

ATTACHMENTS:

- The sender included email attachments that I was not expecting or that makes me want to realize the email message. (This sender doesn't ordinarily include these types of attachments.)
- I see an attachment with a **possibly dangerous file type**. The only file type that is always safe to click on is a PDF file.

CONTENT:

- Is the underlying text to click on a link or open an attachment to avoid a negative consequence, so to gain something of value?
- Is the email not of the sender, or don't I have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illegal?
- Is there an unusual or subtle goal leading about the sender's request to open an attachment or click a link?
- Is the email asking me to click on a compromised or misleading picture of myself or someone I know?

© 2015 Frost Brown Todd LLP. All rights reserved. www.frostbt.com

U.S. COMPUTER CONNECTION
203-356-0444
www.uscomputer.com

Frost Brown Todd LLP
ATTORNEYS

Social Engineering

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

Frost Brown Todd LLP
ATTORNEYS

Social Engineering



Frost
Brown Todd ^{LLP}
ATTORNEYS

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.

Frost
Brown Todd ^{LLP}
ATTORNEYS

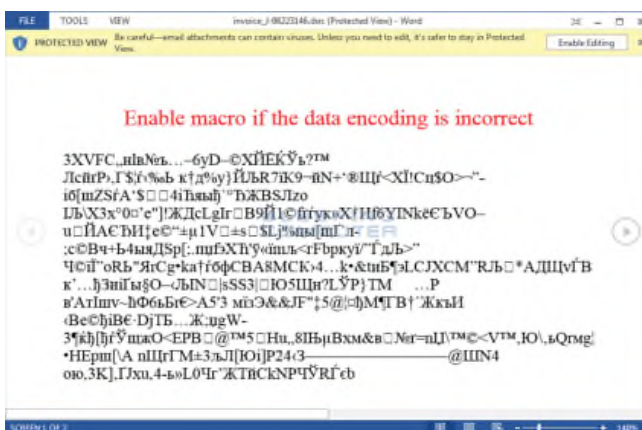
Ransomware

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



Ransomware Example



Ransomware Example

!!! IMPORTANT INFORMATION !!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
 More information about the RSA and AES can be found here:
[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
 To receive your private key follow one of the links:

1. <http://6dbxgqm4crv6r6.tor2web.org/>
2. <http://6dbxgqm4crv6r6.onion.tor2web.org/>
3. <http://6dbxgqm4crv6r6.onion.cab/>
4. <http://6dbxgqm4crv6r6.onion.link/>

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dbxgqm4crv6r6.onion.tor2web.org/
4. Follow the instructions on the site.

!!! Your personal identification ID: [XXXXXXXXXX](#) !!!

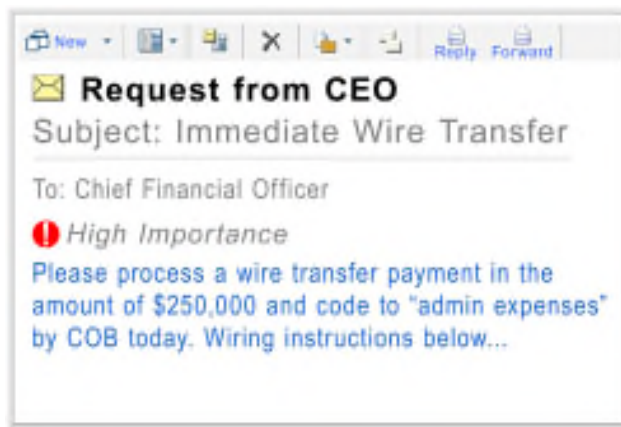
**Frost
Brown Todd**
ATTORNEYS

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.

**Frost
Brown Todd**
ATTORNEYS

CEO Fraud aka Business Email Compromise



CEO Fraud aka Business Email Compromise



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



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



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



- Questions and Comments?
- jshea@fbtlaw.com
- mseverini@fbtlaw.com

