Human Resources, Data Security, and The Internet of Things

Bill Barath
Stephen Reynolds, CISSP, CIPP/US
Ice Miller LLP
DATA SECURITY: TOP THREATS

- Malware
- Lost/Stolen Mobile Devices
- Malicious Insiders
- W-2 Phishing Scams
DATA BREACH: TOP THREATS

“Amateurs hack computers, professionals hack people.”

- Some Hacker
How Are People Hacked?

Hackers try to trick people into ...

- Running the hacker’s malware
- Handing over credentials to the hacker
- Directly working for the hacker
MALWARE

From: Candidate, Joe <joe.candidate@gmail.com>
To: John Doe
Subject: Your personal files are encrypted!

Your personal files are encrypted!

Your important files encryption was produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on 9/15/2013 8:44 PM

Time left 57 : 45 : 37

Next >>
Malware: Most Used Email Lures

Source: ProofPoint, The Human Factor 2016
Morning,

Hope you had a good weekend. Do you have pdf copies of the employees’ W2s? Could you please email them to me for a quick review?

Sent from my iPhone
MALICIOUS INSIDERS
What is the Internet of Things?
The IoT is a growing part of our lives
The IoT is a growing part of business

Internet of Things Devices by Industry

IoT network connections –
2014 vs. 2015 % growth

- Healthcare/Pharma: 26%
- Home monitoring: 50%
- Energy/Utilities: 58%
- Smart cities: 43%
- Agriculture: 33%
- Transportation/Distribution: 49%

Source: Verizon data
IoT Human Resources Considerations

Federal Laws

• Americans with Disabilities Act ("ADA")
• Genetic Information Nondiscrimination Act ("GINA")
• HIPAA/Privacy Laws
• Federal Trade Commission
IoT Data Security and Privacy Concerns
So what can you do?
What to Do?

EMPLOYEE POLICIES/PRACTICES

• Hiring new employees
• Security/Privacy training
• Internet/Email Usage policy
• What occurs at employment termination
• Record retention guidelines
• Bring your own device (BYOD) policy
[COMPANY NAME] grants its associates the privilege of purchasing and using smartphones and tablets of their choosing for work activities. [COMPANY NAME] reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of [COMPANY NAME]’s data and technology. Limited exceptions to the policy may occur due to variations in devices and platforms.

Associates must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.
BYOD Policy

- Acceptable Use
- Devices and Support
- Reimbursement
- Security
- Risks/Liabilities/Disclaimers
What to do for data security

Suggestions for Businesses

• Enforce an effective password policy
• Use two-factor authentication for remote access
• Have an incident response plan
• Protect mobile devices
• Educate employees
For Additional Resources

http://www.icemiller.com/iot-resource-center/

Questions?

Stephen Reynolds, CISSP, CIPP/US
stephen.reynolds@icemiller.com

Bill Barath
william.barath@icemiller.com