

HR's Role in Cybersecurity: Analyzing the "E" in the Employment Environment

2019 GPSHRM Legal Conference

May 8, 2019

By: Jeffrey D. Slanker

Overview

- The scope of the problem
- Data at risk
- Risk factors
- Ways to manage risk through Human Resources
- The intersection of the electronic world and employment issues

Growing Cybersecurity Threats

Symantec Internet Security Threat Report, Volume 24 - 2019

- Formjacking – Large and small businesses such as British Airlines lost millions of dollars in 2018 due to formjacking.
 - British Airlines had 380,000 credit cards stolen, potentially netting more than \$17 million to criminals
- Living-off-the-land (LotL) are now a cyber crime go to
 - Supply chain and LotL attacks have ballooned by 78% in 2018
- Symantec blocks 115,000 malicious PowerShell scripts per month and the use of malicious PowerShell scripts has increased by 1,000% in 2018
- Routers/cameras connected to WiFi fall into 90% of the easily infected device category
- Malicious domains can pose as legit political websites to sway votes through Social Media
 - FaceBook and Twitter fought malicious minions attempting to sway voters
 - 10,000 accounts that were posting messages encouraging people not to vote were removed by Twitter in 2018.

Courtesy of www.symantec.com/security-center/threat-report

Copyright © 2019 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their ISTR respective owners.

WELCOME TO THE DARK NET, A WILDERNESS WHERE INVISIBLE
WORLD WARS ARE FOUGHT AND HACKERS ROAM FREE



By Williams Langwiesche
Vanity Fair- September 2016

Common Types of Attacks

- Identity thieves
- Malware
- Hacking
- Phishing



Courtesy of www.lifewire.com



Courtesy of www.squareup.com



Courtesy of www.izoologic.com

What Sensitive Data do You Maintain?

- Data about your employees and business
 - Personally identifiable information
 - Financial information
 - Health information
 - Confidential information that, if released, could cause personal embarrassment
 - User credentials and passwords
 - Proprietary information and trade secrets
 - Research data information about how networks and IT resources work
- HR data is valuable making it a target

The Human Behavior Risk

- Security has a human component and a technology component
- Obviously, the technology component is going to be governed by information technology and management information system
- People and human errors can be managed though



Courtesy of learnaboutgmp.com

Questions You should be able to Answer

- In Human Resources must have an understanding of how to protect data
 - What and where is my HR data including personally identifiable information?
 - How sensitive is my HR data classified in my organizations' policies and procedures?
 - What are the legal and contractual obligations for protecting my data?
 - Who is responsible for securing my data?
 - Who has access to my data?
 - What do I do when I travel?
 - What do I do if I think someone has accessed my data improperly?

Recognizing Threats

- As a threshold manner, you must have some idea of how to recognize threats or compromises
- Many companies have software system in place to address risk of viruses and cyberattacks
- What remains are attacks that come from outside the organization that rely on a user to permit them access in some way
 - Phishing
 - Malware distributed through e-mails
 - Malicious attacks from employees and former employees
- Inadvertent disclosure and accessing data through insecure networks

An Ounce of Prevention...

- The technology side



Courtesy of www.bookings.edu

- The human side

The Technology Side

- Working with inside/outside information technology personnel to understand how information is stored, protected, and when it is vulnerable
- Making sure that information technology systems are up to date and address vulnerabilities
- Making sure there is a protocol for discovering breaches of data
- Anti-virus systems, spam filters, firewalls, secure networks

The Human Side

- Develop and disseminate information security procedures and protocols including a BYOD policy
- Training all HR staff and employees on cyber security procedures and protocols including data security, restriction, identifying breaches, and avoiding inadvertent disclosure of data.
- Developing an off-boarding process that effectively protects data and making sure that process is followed
- Consideration of discipline for failure to comply with procedures and protocol
- Information security should touch what employees do on an every day basis and be a part or consideration of employees' every day work

Things to do as an HR Professional

- Keep abreast of potential new attacks and methods of attack
- Make sure procedures and protocols are reviewed and updated and trainings are conducted accordingly if there are technological developments and changes
- Make sure that employee roles, with respect to working with data, are clearly defined and limited
- Compartmentalize access to data and restrict as needed

What to do when Subject to an E-mail/Data Breach?

- Protect staff/public. Does the email threat indicate a bigger risk of violence?
- Stop the offending email(s).
- Identify individual(s) responsible. Who was sending the emails?
- Identify where the evidence is located. Which email accounts are involved; is it stored on the server locally, or on a remote email account(s)?
- Protect and preserve evidence. Has it been successfully collected and documented?
- Document steps taken above and why they were taken.

Data Breach Notification Legal Requirements

- **Florida Information Protection Act of 2014**
 - Covered entities
 - Breach
 - Notice Requirements
 - Penalties

When Litigation Hits

- Litigation hold requirements
- Data preservation
- Working with information technology and legal counsel to successfully defend employment actions

Some Common Employment Issues in the E-World

- Wage and hour and electronic devices
- Email and computer systems and union organizing
- Social media, discrimination, and protected activity

QUESTIONS???

SNIFFEN & SPELLMAN, P.A.

123 North Monroe Street
Tallahassee, Florida 32301
Telephone: (850) 205-1996
E-Mail: jslanker@sniffenlaw.com