

CYBERSECURITY

San Diego HR Forum

March 2017

BLAKE HERN

Current: Encore Capital Group, Inc.
Chief Information Security Officer

- Security Architecture
- Risk Management and Governance
- SecOps
 - Threat Prevention
 - Threat Detection
 - Incident Response



Former: KPMG LLP
Risk & Compliance Advisory

- Telecommunications, Financial Services, & Healthcare

AGENDA

- Cybersecurity in the News
 - The Collision of Cybersecurity & Privacy
 - Privacy in the Workplace
 - Take Away Items/Thoughts for the HR Professional
-

CYBERSECURITY HOT TOPICS

WIKILEAKS RELEASE ON MARCH 7TH

- “By the end of 2016, the CIA's hacking division, had over **5000 registered users** and had produced more than a thousand hacking systems, trojans, viruses, and other **"weaponized" malware**. Such is the scale of the CIA's undertaking that by 2016, its hackers had utilized more code than that used to run Facebook.”
-

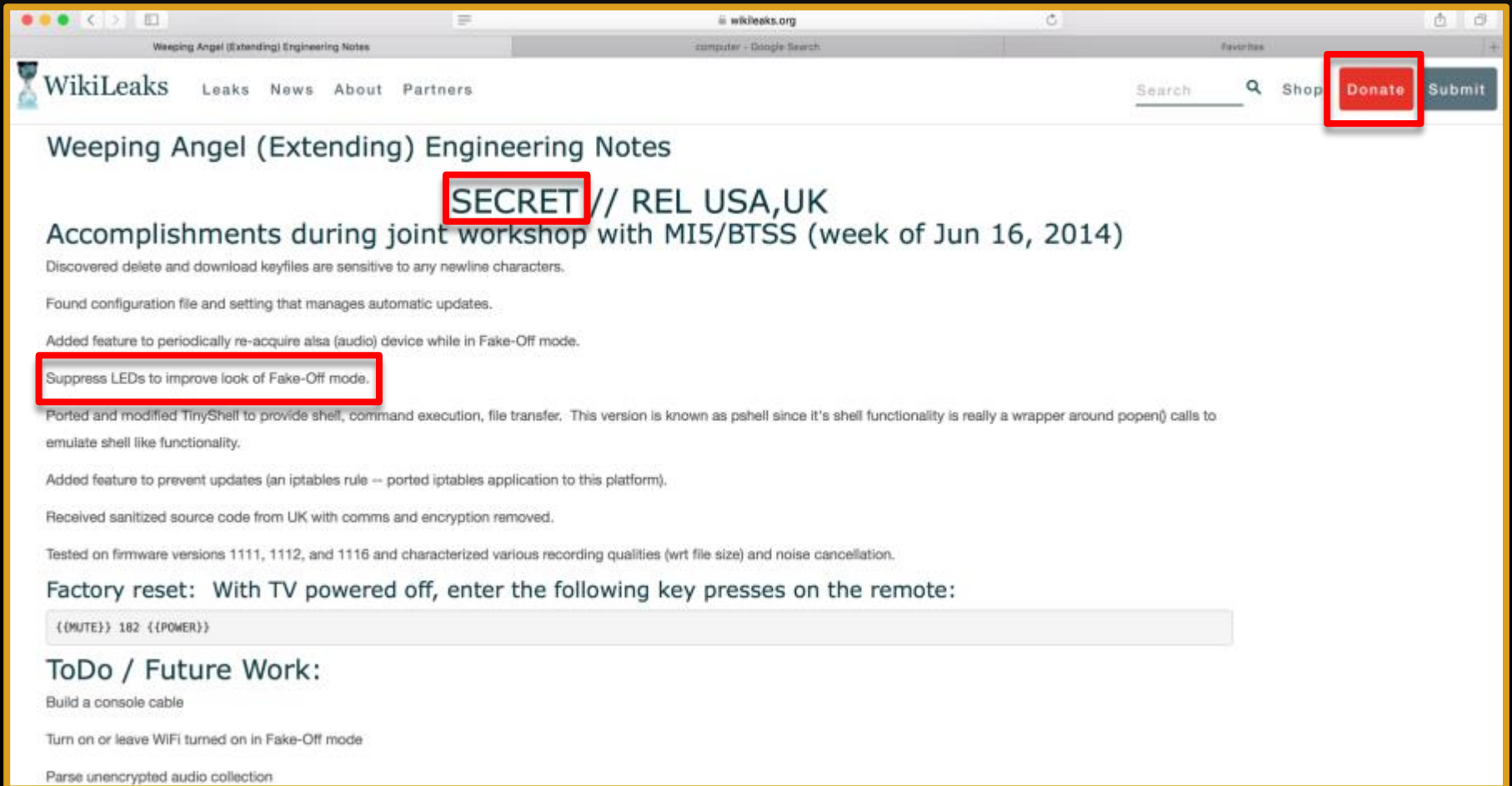
CODE NAME "VAULT 7": THE CIA'S CYBER ARSENAL



Cyber
Weapons



THE WIKILEAKS SITE



The image is a screenshot of a web browser displaying the WikiLeaks website. The browser's address bar shows 'wikileaks.org'. The page title is 'Weeping Angel (Extending) Engineering Notes'. The WikiLeaks logo is in the top left, and navigation links for 'Leaks', 'News', 'About', and 'Partners' are in the top center. On the top right, there are links for 'Search', 'Shop', 'Donate', and 'Submit'. The 'Donate' button is highlighted with a red box. The main content of the page is a document titled 'Weeping Angel (Extending) Engineering Notes'. The document is classified as 'SECRET // REL USA, UK', with 'SECRET' highlighted in a red box. The document content includes several bullet points: 'Discovered delete and download keyfiles are sensitive to any newline characters.', 'Found configuration file and setting that manages automatic updates.', 'Added feature to periodically re-acquire aisa (audio) device while in Fake-Off mode.', 'Suppress LEDs to improve look of Fake-Off mode.' (highlighted in a red box), 'Ported and modified TinyShell to provide shell, command execution, file transfer. This version is known as pshell since it's shell functionality is really a wrapper around popen() calls to emulate shell like functionality.', 'Added feature to prevent updates (an iptables rule -- ported iptables application to this platform).', 'Received sanitized source code from UK with comms and encryption removed.', and 'Tested on firmware versions 1111, 1112, and 1116 and characterized various recording qualities (wrt file size) and noise cancellation.' Below this, there is a section for 'Factory reset: With TV powered off, enter the following key presses on the remote:' followed by a code block containing '{(MUTE)} 182 {(POWER)}'. At the bottom, there is a 'ToDo / Future Work:' section with items: 'Build a console cable', 'Turn on or leave WiFi turned on in Fake-Off mode', and 'Parse unencrypted audio collection'.

WikiLeaks Leaks News About Partners

Search Shop **Donate** Submit

Weeping Angel (Extending) Engineering Notes

SECRET // REL USA, UK

Accomplishments during joint workshop with MI5/BTSS (week of Jun 16, 2014)

Discovered delete and download keyfiles are sensitive to any newline characters.

Found configuration file and setting that manages automatic updates.

Added feature to periodically re-acquire aisa (audio) device while in Fake-Off mode.

Suppress LEDs to improve look of Fake-Off mode.

Ported and modified TinyShell to provide shell, command execution, file transfer. This version is known as pshell since it's shell functionality is really a wrapper around popen() calls to emulate shell like functionality.

Added feature to prevent updates (an iptables rule -- ported iptables application to this platform).

Received sanitized source code from UK with comms and encryption removed.

Tested on firmware versions 1111, 1112, and 1116 and characterized various recording qualities (wrt file size) and noise cancellation.

Factory reset: With TV powered off, enter the following key presses on the remote:

```
{(MUTE)} 182 {(POWER)}
```

ToDo / Future Work:

- Build a console cable
- Turn on or leave WiFi turned on in Fake-Off mode
- Parse unencrypted audio collection

SO...WHEN DID OUR FIGHT FOR
PERSONAL LIBERTY BECOME A
FIGHT FOR PRIVACY?

AMENDMENT IV

PRIVACY OF THE PERSON AND POSSESSIONS

The right of the people to be secure in their **persons**, houses, papers, **and effects**, against **unreasonable searches and seizures**, shall not be violated, and no Warrants shall issue, but upon **probable cause**, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

SO...WHERE DO WE WILLINGLY
GIVE UP SOME OF OUR ONLINE
(OR CONNECTED) PRIVACY?

THE WORKPLACE

RAISE YOUR HAND, IF YOU HAVE...

- Checked **health records** or **insurance** claims at work?
- Synced you **FitBit** to your company mobile phone or laptop?
- Created or edited your **resume** on your work computer?
- Completed your **taxes** on your work computer?
- Accessed your **paystub**, W-2 forms, or stock plan details on your work computer?
- Checked your personal bank account balance, looked at your online stock portfolio, or any other **personal financial sites**?
- Accessed a social media or **dating site**?

Your IT
Department
may have
seen all
of it

ANALYZING USER BEHAVIOR

- **Email analysis**
 - Karen sends 2MB of outbound email per day
 - Over the past week, she has averaged 5M per day
 - She could be stealing data
 - More likely...she's about to give her 2 weeks notice
 - **Web traffic analysis**
 - LinkedIn: updating your profile
 - Facebook: friend analysis, sentiment analysis through text analysis
 - CareerBuilder.com
 - jobs.ABCcompany.com
 - Religious or political group websites
-

ANALYZING USER BEHAVIOR

- **File Analysis**
 - Editing a document called “Hern-Resume.doc”
 - **GPS Analysis**
 - Laptops, Smart Phones, Health Devices
 - Who from the office hangs out together outside of work?
 - Where and how long did an employee go out to lunch?
 - **Sensor Analysis**
 - Seat Sensors used by Facilities Departments
 - Web Cams to assess employee engagement
-

ANALYZING USER BEHAVIOR

- **Public Records**
 - Eviction Notices
 - Lawsuits
 - Personal Matters
 - Bankruptcies and debts
- **Infinity Screening**
 - “empower employers to proactively identify factors which increase their risk to negligent retention claims, workplace violence, loss due to internal shrinkage and public embarrassment through negative publicity”
 - What do you do, when you get a “red”?



BECOMING PROACTIVE

- Two employees of Vanderbilt University Medical Center have been discovered to have inappropriately accessed the medical records of more than 3,000 patients.


While the HIPAA Security Rule requires audit logs to be regularly reviewed by HIPAA-covered entities, in this case the inappropriate accessing of ePHI continued for 19 months before it was detected.

**Anomaly Detection &
User Behavior Analytics
are the future of Corporate Information Security**

**TAKEN FROM MY
LINKEDIN FEED THIS
PAST WEEK**

AT&T LTE 4:43 AM 97%

People are talking about



Learn How-to Gather Intelligence Online
mcafeeinstitute.com

Justice Simone
Coach & Trainer at McAfee Institute & L...
Save 68% OFF, 3 seats left! Enroll today.
1 Like

Like Comment Share

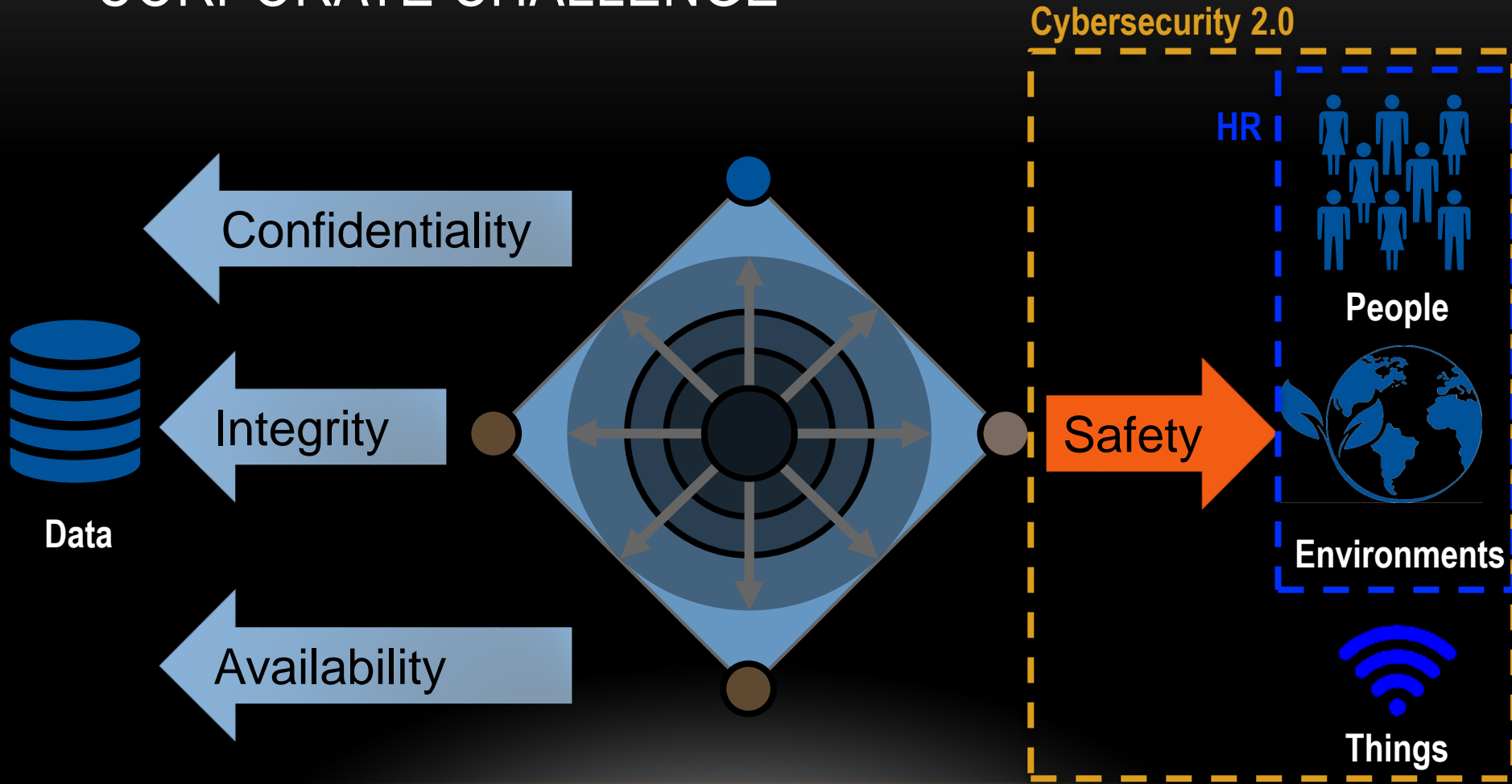
Michael Bradshaw CCII. CPCI

Home My Network Messaging Notifications Jobs

Questions for the HR Professional...

- ① How do you feel about your IT Administrators and Security Teams knowing all of these personal things about you?
- ② Have you put in the policies and protocols to control for analyzing your personnel (i.e. UBA)?
- ③ Should your employees expect any rights to privacy? Or, did they sign away their privacies?

CYBERSECURITY IS FACED WITH A NEW CORPORATE CHALLENGE



TAKE-AWAYS FOR THE HR PROFESSIONAL

Compensation & Benefits

Strategic Initiatives

Talent Acquisition

Learning & Development

Employee Relations

Health & Safety

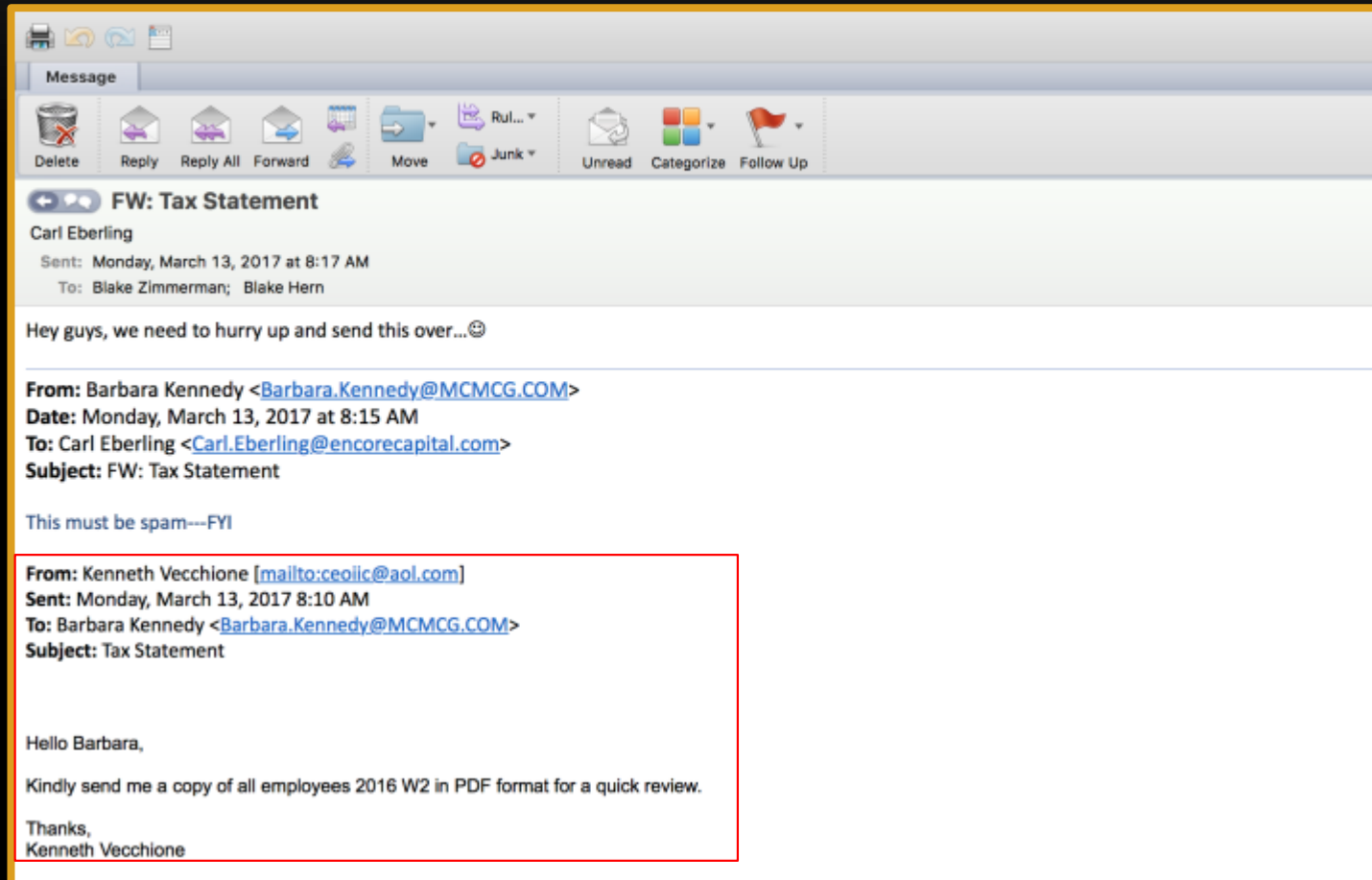
HR Business Partners

HRIS

HR DEPARTMENTS ARE A LEADING SOURCE OF ACCIDENTAL DATA LOSS

- From February 2017:
 - According to the letter, the breach occurred on Nov. 21, 2016 after a Boeing employee encountered a formatting issue and **emailed a spreadsheet to his spouse who didn't work at the company**. The file contained sensitive, personally identifiable information of 36,000 of the aircraft manufacturer's employees. The file included the names, places of birth, BEMSID, or employee ID numbers, and accounting department codes. The spreadsheet also included Social security numbers and dates of birth, albeit in "hidden columns," according to Olson.
- From October 2016:
 - The Confidential Alpha Roster (MIRS report) that contains **all staff names, social security, dates of birth**, and other non-confidential data such as classification, tenure, and time base had been saved in a non-secure location, accessible to all Folsom State Prison Staff.

HR SPEAR PHISHING EXAMPLE




HOW MUCH CAN YOUR COMPETITORS GLEAN FROM PUBLICALLY ACCESSIBLE DATA?

- **LinkedIn**
 - “lead mergers and acquisitions due diligence efforts to assess talent and opportunities for efficient consolidations”
- **Facebook**
 - Counterintelligence through picture locations and check-ins
- **Hub-and-Spoke**
 - You become a target for a treasure trove of personnel information

Talent Acquisition

- Don't trust your screens – some candidates have gamed the system
- There is about to be a huge shortage of cybersecurity professionals, and most candidates won't be qualified
- What will be your willingness and allowance to leverage new types of data when vetting a client (e.g. Facebook friend analysis)?

Learning & Development

- With the convergence of personal devices into the workplace, where should security awareness training start and end?
 - Training must transcend the “check-the-box” CBTs and utilize simulation trainings
 - Should your HR Department have a “Cybersecurity Lead” to stay out in front of these emerging items?
- 

Health & Safety

- Are you prepared to corporately respond to a threat against critical infrastructure?
 - Water Systems
 - Transportation Systems
 - Electrical Systems

HR Business Partners

- Where can a business process be improved with the use of tools originally designed for cybersecurity?
 - Sensor Data
 - Web Analytics
 - Log Analysis
- Could the cybersecurity tools become a strategic advantage for your company?

HRIS

- Criminal hackers are seeking opportunities for exploitation – exploitation of:
 - Health records
 - Compensation data
 - Hierarchy data
- HRIS professionals need to have cybersecurity training because...you may be a path of least resistance

Employee Relations

- Privacy for employees...do they get it?
- Policies for IT's permissible use and viewing
 - Most IT Departments can at least monitor the following:
 - Web Traffic
 - E-mail Traffic
 - File Use & Storage
 - Removable Media Use & Storage
 - Login, Logout, & System Use

FINAL WORDS

- Your IT and Information Security Team has a **powerful toolset**
 - What policies and protocols **govern** their use of these tools?
 - How much, if any, **privacy** can an employee expect in the workplace?
 - Can these tools be **leveraged** for the betterment of HR and business operations?
 - Do you have a healthy dose of **paranoia** by now?
-