

Employee Surveillance and Cybersecurity: How to Protect Your Company

IECRM

October 4, 2018



*Hot Industry.
Cool Career.*



Presented by:

Danielle Urban

Phone: (303) 218-3654

Email: durban@fisherphillips.com

THE THREATS

- External theft and threats
 - Hacking; phishing; malware; ransom
- Internal theft and threats
 - Employee defections
 - Negligence



Increasing Cyber Attacks and the Elusive Insider Threat

- Social Engineering: psychological manipulation of people into performing actions or divulging information
 - Pretexting
 - Phishing
 - Baiting



What's at stake? – Business & Employee Information

- Supply chain operations and production timeframes
- Vendor list
- Customer information
- Employee information: SSNs; Contact Information; Health Information; Financial Information; Insurance Information; Background Check; Drug Testing; Personnel Records; Personal Family Information.
- Contract terms and pricing
- Pricing strategies
- Sales and marketing strategies
- Product roadmaps / development plans / features / architectures
- Merger and acquisition insights
- Meetings, conferences and business/social networks



Ransomware

- Originally designed to lock down victim's data until ransom is paid
- Now, attackers threaten to disclose data if victim doesn't pay up
 - Netflix
 - Disney
 - Hospitals and clinics



Phishing Attacks

- Emails or links to unwitting employees
- Particularly common in first quarter
- Attacks are launched on employers of every size.



Phishing Attacks

- Unwitting disclosure of confidential employee information
- Training and prevention key
- In the event of a breach, have a plan
 - Notification laws
 - Mitigation
 - Investigation



Protecting Your Company

- Vulnerability assessments
- Penetration assessments
- Emergency Response Plan
- Employee training
- Cyber insurance



INTERNAL THREATS



Employee Defections: Critical Steps

- Contractual Restraints
 - Come in all shapes and sizes:
 - Non-compete agreements
 - Non-solicitation agreements
 - Confidentiality agreements



Employee Defections: Critical Steps

- Opportunities to be proactive:
 - Policies/procedures
 - Confidentiality; BYOD; Handling
 - Trade secret audits
 - Exit interviews
 - Reminder/demand letters
 - Severance agreements
 - Employee relationships

Prevent Insider Data Theft

- Employee electronic messages both outgoing and inbound should be monitored.
- Trade Secret & Personal Information should be encrypted.
- Employees should be trained in Info Sec and Social Engineering attacks.
- Anonymous information line to report suspicious activity should be implemented.
- Conduct third party reviews and penetration testing as well as risk and vulnerability assessments to keep honest employees honest, and make it so hard to steal that employees will not attempt to compromise the system.
- Develop policies and procedures and have employees sign the documents.

Prevent Insider Data Theft

- Establish Strong Passwords
- Limit use of flash drives
- Restrict access to personal data and trade secrets
- Prohibit usage of unauthorized applications (e.g., Dropbox)
- Utilize physical controls
- Track usage (and make sure employees know it)



Prevent Insider Data Theft

- Deploy two-factor authentication mechanism
- Implement physical access controls & barriers to disclosure
- Integrate an intrusion detection infrastructure
- Shred confidential discarded documents, erase tapes thoroughly
- Deploy surveillance devices
- Employ anti-deletion mechanisms
- Perform regular data backups
- Utilize network, not local hard drive, space





EMPLOYEE MONITORING



Why Monitor?

- To protect trade secrets and confidential information
- Productivity
- To prevent harassment/discrimination
- Minimize risk of data breaches
- Track location of company equipment
- Workplace safety
- To prevent other illegal activities



Employee Background Checks

- According to one survey, 92% of employers subjected some or all job candidates to criminal background checks
- **But why?**
 - To prevent theft and fraud
 - To prevent workplace violence
 - To avoid liability for negligent hiring
- **Potential Problems**
 - Increased EEOC scrutiny
 - The rise of FCRA Class Actions

Technology Used by Employers to Monitor Employees

- Biometrics
- E-mail monitoring
- Social media
- GPS technology
- Cell phone monitoring
- Key logging
- Fitness trackers (Fitbit, Nike+FuelBand, Jawbone, UP)



GPS Technology

- Common Monitoring Techniques
 - Placing a GPS tracker on a company-issued vehicle
 - Issuing company-owned smart-phones with GPS tracking capabilities
 - Placing trackers on personally-owned vehicles used in work-related activities



GPS Technology

- Address employee privacy concerns
 - Give notice of GPS tracking to employees
 - Limit the use of GPS trackers to company-owned property
 - Use GPS tracking for a specific purpose
 - Only collect/store information that impacts job performance



Bring Your Own Device Policies

- Authorize employees to use personal electronic devices to conduct business
- Can provide key benefits, such as increased productivity, reduced IT costs, and better mobility for employees
- Increases risk of data breaches and liability from such breaches
- Increases risk of spoliation of evidence and makes preservation more difficult to manage and enforce



BYOD Security Best Practices

- Use password protected access controls
- Control wireless network and service connectivity
- Control application access and permissions
- Keep operating system, firmware, software, and applications up-to-date
- Back up device data



BYOD Security Best Practices

- Enroll in “Find my Device” and remote wipe services
- Never store personal financial data on a device
- Beware of free apps
- Run mobile antivirus software or scanning tools
- Use Mobile Device Management (MDM) software as recommended by IT
- Develop comprehensive policies

The Changing Data Privacy Landscape and Compliance

- Colorado's new data privacy law
- The California Consumer Protection act takes effect on January 1, 2020
- 50 states – 50 different laws regarding data breach

Thank You



Presented by:
Danielle Urban
Phone: (303) 218-3654
Email: urban@fisherphillips.com