# PEO University

# Cybersecurity for PEOs


Joe Lazzarotti
Jackson Lewis P.C.
Joseph.Lazzarotti@jacksonlewis.com
(813) 512-3225

John Ykema
eEmployers Solutions, Inc.
jykema@eesipeo.com
(832) 725-5000

Usama Kahf
Fisher Phillips
ukahf@fisherphillips.com
(949) 798-2118


Sponsored by:





## Agenda

- Top Threats – What's at Stake
- Legal Landscape on Cybersecurity
- Reasonable Security Measures
- Prevention and Response Strategies – Be Proactive
- Cyber Insurance Planning

Sponsored by:

© Copyright 2024 National Association of Professional Employer Organizations

# Common Threats

- Ransomware
- Phishing / Smishing
- Payment Scams
- Internal Threats
- Carelessness
- Data Stored on Personal Devices
- Vendor Security


Sponsored by: blr GP solved MSA SLAVIC 401K





# Common Threats - Ransomware

Source: Microsoft stock images.

**Current Ransomware Trends**

- Supply chain attacks
- Double extortion
- Ransomware as a service (RaaS)
- Attacking unpatched systems

Source: techtarget.com

Sponsored by: blr GP solved MSA SLAVIC 401K

# Common Threats – Insider Threats

Disgruntled Employee

Internal Carelessness

Source: Microsoft stock images.







# Theft of Employee Information

- How is it being used?
  - When incidentally embedded in confidential or trade secret information being misappropriated by a departing employee.
  - Financial fraud, including tax fraud.
- Potential liability
  - Some consumer privacy laws treat employees like consumers, meaning heightened notification standards.
  - Under new consumer privacy laws, an organization may be held liable for failure to put in place appropriate security measures.
  - Civil actions, including class action lawsuits.
  - Regulatory investigations and penalties.

# Common Threats – Data on Personal Devices

- Allowing employees to use personal devices for work purposes can provide key benefits, such as increased productivity, reduced IT costs, and better mobility for employees.
- However, this increases risk of data breaches and liability from such breaches.
- This increases risk of spoliation of evidence in the event of litigation and makes preservation more difficult to manage and enforce.







# Common Threats – Trusted Vendors

Source: Microsoft stock images.

- What outside vendors does your organization rely on?
  - Payroll
  - Benefits
  - CRM
  - Etc.
- According to a 2019 eSentire survey, for nearly half of all orgs that experienced a data breach, it was caused by a third-party vendor.

https://blog.rsisecurity.com/why-perform-a-vendor-cybersecurity-assessment/

# What do courts consider to be reasonable security measures?

- Industry custom
- Violation of a statute, regulation or ordinance
- Poor implementation of a security control or failure to implement
- Intervening criminal act vs. foreseeable attack




Source: The Sedona Conference, *Commentary on a Reasonable Security Test*, 22 SEDONA CONF. J. 345 (2021).







# Data Breach Response

- What constitutes a security incident?
  - Report of a physical or criminal act (e.g.: theft of a computer, laptop, tablet or phone)
  - Suspicion that a device has been compromised to allow access to sensitive data
  - Security issue with a person using equipment
  - Other circumstances that warrant investigation include disruptive viruses, denial of service attacks, malware, phishing scams, etc.

# Data Breach Response

1. Investigate and secure the data
2. Immediately involve cybersecurity expert and legal counsel
   - Report to cyber insurance carrier
3. Identify applicable state and federal laws
4. Determine if a "breach" has occurred as defined by applicable laws
5. Determine if notification is required under applicable laws
   - Who should be notified?
   - When to notify?
   - Contents of notice
6. Follow-up risk mitigation steps







# Data Breach Response

- State laws vary in 6 areas:
  1. Scope of Covered PII
  2. Trigger for Notification Obligation
  3. Recipients of Notice
  4. Content of Notice
  5. Timing of Notice
  6. Enforcement

# Prevention and Pre-Incident Strategies

- Annual security reviews
- Security assessments
- Regularly update your information security policy
- Annual cybersecurity trainings
- Develop business backup and continuity practices
- Obtain and maintain cyber insurance









# 10 Steps for PEOs to Manage Cyber Risks

1. Obtain Executive Support
2. Assign Responsibility
3. Know Your Business
4. Know Your Data
5. Know Your Insurance
6. Know Your Vendors
7. Assess Your Risks, Drive Compliance
8. Develop Incident Response & Business Continuity Plan
9. Training & Awareness
10. Periodic Review

# Best Practices for Cyber Insurance Underwriting

- Business Continuity / Disaster Recovery
- Biometric Information (Policy Review)
- Credit Cards (PCI-DSS Compliance)
- Multi-Factor Authentication (MFA)
- Encryption
- Scanning Emails for Ransomware and Malicious Attachments
- Endpoint Detection and Response (EDR)
- Backup
- Social Engineering / Phishing Training
- Wire Transfers and ACH Protocols







# QUESTIONS?

# THANK YOU!


- Joe Lazzarotti
- Jackson Lewis P.C.
- Joseph.Lazzarotti@jacksonlewis.com
- (813) 512-3225

John Ykema
eEmployers Solutions, Inc.
jykema@eesipeo.com
(832) 725-5000

Usama Kahf
Fisher Phillips
ukahf@fisherphillips.com
(949) 798-2118


Sponsored by: