Bond

Manufacturing Week
Webinar Series
October 2-6, 2017

Cybersecurity: What We Should Be Doing

Presented by Michael D. Billok

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond

Bond

Manufacturing Week Webinar Series October 2-6, 2017

October 2: Cybersecurity: What We Should Be Doing

October 3: Protecting Your Manufacturing Business from IP Theft

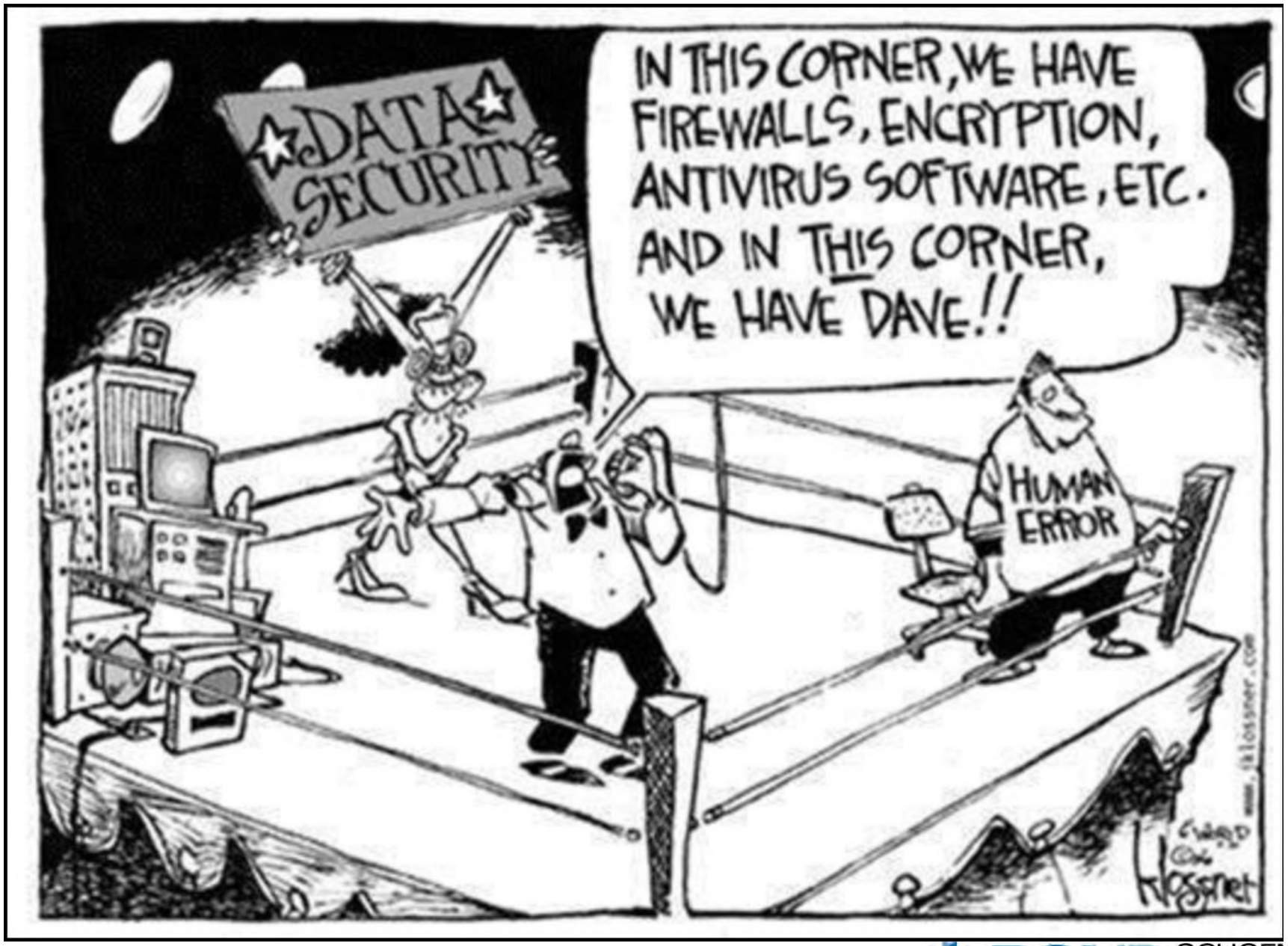
October 4: Wage and Hour Traps for the Manufacturing Industry

October 5: Avoiding OSHA Liabilities

October 6: Navigating Immigration Issues Within the Manufacturing Industry

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond



BOND SCHOENECK & KING ATTORNEYS

Federal Trade Commission (FTC) Oversight

- FTC oversees cybersecurity under Section 5 of FTC Act governing enforcement of **unfair** and **deceptive** commercial practices

  "What is reasonable and appropriate is a question that encompasses the totality of the circumstances in which a company operates. Based on our law enforcement experience regarding data security, the FTC has recognized there is no 'one size fits all' security plan. Increased levels of information sensitivity require increased protection." (In the Matter of Cyber Security Certification Program, PS Docket No.10-93)

(cont'd)

Federal Trade Commission (FTC) Oversight

- Major FTC Enforcement Actions:
  - GMR (2015) – Failure to manage third party contractors
  - BJ's Warehouse (2008) – Failure to dispose of data
  - Eli Lily (2002) – Failure to provide employee training and oversight

FTC “Unfair” Standard

- FTC v. Wyndham Worldwide Corporation (Third Cir. 2015)
  - Affirmed FTC oversight and jurisdiction
  - Held that Wyndham had notice of standards to which it would be accountable to the FTC
  - Violations of FTC standard— “unfair” practice— included:
  - Failed to encrypt stored credit card information;
  - Did not use industry standard password complexity;
  - Did not use reasonable measures to detect and prevent authorized access; and
  - Failed to address identified security issues

“Deceptive” Practices

- *In the Matter of Dwolla, Inc.*
  - Company had represented in advertisements and elsewhere that its security practices “set[] a new precedent for the industry for safety and security,” and that consumer data was “securely encrypted and stored” in a “bank-level hosting and security environment.”
  - It also represented that its security procedures were “PCI (Payment Card Industry) compliant.”
  - The representations were false. In reality, the security procedures that were being employed fell far short of industry standards, did not encrypt consumer data, and were not PCI compliant
  - *No consumer data was actually exposed*

State Oversight: SSNs in NY

- N.Y.'s Social Security Protection Law prohibits:
  - Disclosure of SSNs to the public
  - Printing SSNs on cards or tags
  - Encoding or embedding SSNs on card or document
  - Requiring transmission of SSN over internet
  - Requiring use of SSN to access web site
  - Printing SSN on materials sent by mail
- Subject to various exceptions

(cont'd)

8

State Oversight: SSNs in NY

- This statute also requires safeguarding SSNs in your possession
  - "Reasonable measures" to limit access
  - Provide "necessary" and "appropriate" safeguards to protect confidentiality
- Penalties for violating this statute may be as high as $250,000

(cont'd)

State Oversight: SSNs in NY

- Takeaways
  - *Encrypt SSN data wherever possible*
  - Ensure you have adequate cybersecurity policies and procedures in place
  - Limit access to SSNs
  - Review your use of SSNs on cards, documents, etc.
  - If you have employees in other states, consider legal requirements of those states

10

State Data Breach Laws

- 48 States*, DC, Guam, Puerto Rico and the Virgin islands now have legislation requiring entities to notify individuals (and often certain other parties) of security breaches involving “personally identifiable information”
- *No notification statutes currently in Alabama or South Dakota
- Laws are constantly changing
- Multistate clients can be subject to multiple differing requirements

NYS Information Security Breach and Notification Act (Gen. Business Law §899-aa)

- Who must comply?
  - State entities, individuals, and businesses that own, operate or maintain computerized data that includes private information
- What private information is covered?
  - Social Security numbers, drivers license number, credit card or financial account information in combination with pass/security code to the account

(cont'd)

NYS Information Security Breach and Notification Act (Gen. Business Law §899-aa)

- What is the duty to notify?
  - Notice to those whose information is disclosed without unreasonable delay or immediately to the organization that provided the data
  - Specifies methods of notice—mail, electronic (if consented to), phone (if logged)
  - May be substitute notice (posting, media) if can justify high cost of individual notice to AG (more than $250,000, or 500,000 people)
  - If notice provided to any NYS residents, duty to notify the State AG, Consumer Protection Board, and State Office of Cybersecurity

(cont'd)

NYS Information Security Breach and Notification Act (Gen. Business Law §899-aa)

- Such notice shall include:
  - Contact information for the person or business making the notification;
  - Description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired
  - These are ***New York's*** requirements. Personal information of other states' residents covered by those state laws—50-state patchwork

Risk Assessment

- What sensitive information does the organization create, use, transmit or store?
- Identify most likely risks and vulnerabilities:
- Means of access to that information;
- How information flows through the organization;
- All devices that access confidential information;
- Consultants and vendors; and
- Human, environmental and natural threats
- Assess the severity of the impact of potential security breach
- Assess security systems and practices in place
- Tailor risk remediation and management based on gap analysis to set priorities and goals

Workforce: Policies and Safeguards for Data Access

- Develop policy to limit access to sensitive data to employees who need access based on job responsibility/title
- Set up process to determine who should have access
- Adopt procedures and systems to restrict access to level of authorization granted
- Monitor access
- Implement procedures to restrict access upon employee termination

Workforce: Training, Policies, and Enforcement

- Training and Awareness
  - For new employees and periodically
  - Consistent, actionable reminders
  - When systems change, technology changes, or new threats arise
- Employee Policies and Sanctions
  - Require employees to acknowledge receipt of security obligations or policies
  - Inform employees that violation can lead to discipline
  - Adopt process for sanctions and tie sanctions to severity of actual and potential harm and intention

Assigned Security Responsibility

- Accountability and Authority in a Security or Senior Officer
  - Does the individual have sufficient training, authority and resources?
  - What is the reporting line to the CEO/President or other senior officer?
  - Does the individual report to the Board periodically?
  - Is the person integrated into business decisions and transactions?
  - Does the individual have access to needed legal and technical resources?

Third Party Agreements

- Prudent business practice prior to sharing any sensitive information
- **Among other provisions:**
  - Obligate the party receiving the data to comply with standards your organization must meet;
  - Require notice to your organization and an investigation in event of breach;

(cont'd)

Third Party Agreements

- **Among other provisions:** (cont'd)
  - Indemnification – allocate responsibility for cost of notice, remediation, etc.;
  - Specify minimum necessary security practices (e.g., encryption);
  - Specify obligations in relation to any subcontractors;
  - Require return or destruction of sensitive data/information at end of underlying agreement; and
  - Right to audit security practices and systems

Examples of Cybersecurity Policies

- Electronic system/acceptable use
  - Passwords
- Mobile devices
- Termination procedures
- Data breach plan

Acceptable Use Policy

- Require employees to lock computer when they step away
- Clarify that no expectation of privacy
- Define unauthorized access
  - Ban use of other employees' passwords
- Restrict employees' access to data
- Impose limits for external media devices
- Limit downloads from third parties

(cont'd)

Acceptable Use Policy

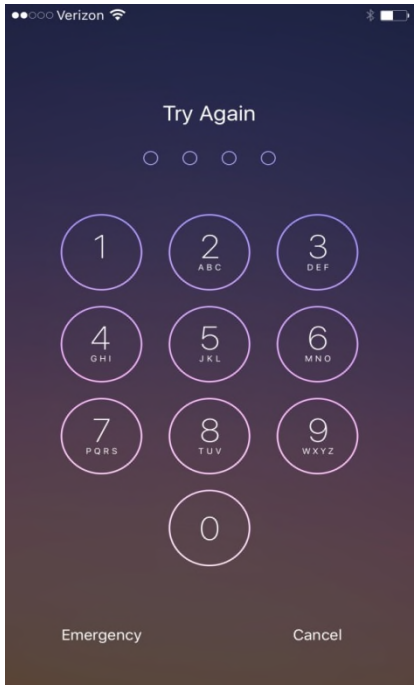
- Impose rules about printed electronic information
  - Sensitive printouts cannot leave workplace
  - Sensitive printouts must be shredded
- Reporting procedure for suspicious activity
- Consider:
  - Restricting personal use of company's system
  - Restricting access to certain websites (e.g., personal e-mail sites – Gmail, Hotmail, etc.)

Password Policy

- Impose strict rules about password strength
- Require frequent changing of passwords
- Consider multi-level system access, especially for remote access
- Require employees to use unique passwords for system and any other devices with company data

Mobile Device Policy

- Require employees to auto-lock device with unique password and to encrypt data
- Create procedure for promptly reporting lost/stolen devices
- Consider software that permits employer to access phone
- Prohibit public Wi-Fi use (coffee shops, hotels, airports)



BOND SCHOENECK & KING ATTORNEYS

Violations → Discipline

- Require employees to acknowledge receipt of security policies
- Require employees to acknowledge completion of training on these policies
- Inform employees that violation can lead to discipline

Suspension/Termination Procedures

- Create procedures for handling employees' data access
  - Turn off system access before suspension or termination is disclosed
  - Ensure recovery of all laptops, mobile devices or other devices with company data
  - Check e-mails sent and documents printed or downloaded prior to suspension or termination

Create Data Response Plan Before An Attack

- Appoint employee to lead in the event of breach
- Identify who should be contacted (management, outside counsel) and how will they be contacted
- Plan how to preserve data related to the intrusion in a forensically-sound matter
- List notification procedures
  - Most states have breach notification laws with varying requirements

Encryption Safe Harbor Rule

- N.Y.’s data breach statute does not apply if information was protected by encryption, unless the encryption key was also acquired/stolen
- Personal information should be encrypted

Cybersecurity Training

- Training on policies and procedures
- Training on how employees can accidentally cause data breaches
  - Loss of external media devices
  - Clicking on a link or downloading attachment to malicious e-mail
  - Inadvertently sharing hidden data
- Team up with IT

Ongoing Process

- Regularly review policies and procedures for potential improvements
- Regularly train current employees
  - Train all new employees
- Monitor compliance with procedures
- Test employees' responses

Takeaways

- Encrypt, encrypt, encrypt
- Review current practices for protecting employee data
- Revise or create cybersecurity policies
- Monitor compliance
- Train employees regularly
- If breach happens, coordinate to find out extent of breach and to send required notices

The information in this presentation is intended as general background information on labor and employment law. It is not to be considered as legal advice. Employment law changes often and information becomes rapidly outdated.

BOND SCHOENECK & KING ATTORNEYS

Cybersecurity: What We Should Be Doing

Michael D. Billok

268 Broadway
Saratoga Springs, NY 12866
518.533.3236
mbillok@bsk.com

REGISTER FOR TOMORROW'S WEBINAR: BSK.COM/#EVENTS