What Data?
I’m A Trucking Company!

Presented by: **Marc C. Tucker**
434 Fayetteville Street, Suite 2800
Raleigh, NC, 27601
919.755.8713
marc.tucker@smithmoorelaw.com

Presented by: **Rob D. Moseley, Jr.**
2 West Washington Street, Suite 1100
Greenville, SC
864. 751-7643
rob.moseley@smithmoorelaw.com
WEBINAR ROADMAP

• Data, What Data?
• Company Best Practices
  • Preparation
  • Response
• Cybersecurity Insurance
• Contracting Considerations
WHAT, ME?

• I don’t have to worry about a data breach because…
  • I don’t have any data
  • My data is safe, it is in the "cloud"
  • I am a small, local business, not a Target or Sony
  • Nobody will want my data
  • I have a firewall to protect my data
  • I outsource my IT
WHY YOU!

The notion that you are too small or too boring is a false sense of security
WHY YOU!

• Data in any form has value to someone, and no business is immune from a potential breach.

• Hackers compromise nearly 30,000 websites each day. A majority of these breaches result from weaknesses in our collective cyber behavior rather than through nefarious means.

• According to the FBI, 90% of cyber-attacks involve phishing email scams that require employee action to succeed.
TRANSPORTATION DATA

• Data intensive industry
  • Customer Information
  • Capacity Information
  • Pricing Information
  • Fleet maintenance
  • Fleet Management
  • Driver compensation analytics
TRANSPORTATION DATA

• The collection and use of data is accelerating
  • Optimizing routes
  • Optimizing loads
  • Managing inventory
  • Fleet maintenance
  • Increasing safety
TRANSPORTATION DATA

- Employee Information
  - Social Security
  - Birthdate
  - Driver’s license
  - Address
  - Phone number
- Wellness Program
  - Personal health information
- Driver qualification files
TRANSPORTATION DATA

• E-commerce is growing
• More and more paper conduits are shifting to electronic
• Can your business survive without this information?
BEST PRACTICES PREPARATION

• Data security is not an IT issue, it is a company issue
  • IT may manage the “nuts and bolts” of network systems; however, all employees must be responsible for the use and protection of information
  • Improper use or disclosure of information will impact the company, not IT
• What are your client or customer expectations?
• Ignoring data security issues outside of IT is a recipe for disaster
BEST PRACTICES PREPARATION

• Potential sources of a data breach
  • Employee error
  • Phishing and malware scams
  • Stolen, lost, or unattended computer
  • Stolen, lost, or unattended smartphone or tablet
  • Hacking incidents
  • Malicious employee
  • Unknown intrusions
BEST PRACTICES PREPARATION

• Minimize Your Risk of Exposure
  • Establish policies and procedures
  • Identify what data you have
  • Know where that data is stored
  • Identify all individuals with access to your data
  • Determine what and when data can be destroyed
  • Proactively monitor and train employees
  • Designate a data security officer
  • Conduct periodic security testing and compliance
BEST PRACTICES PREPARATION

• What Data Do You Have?
  • Employee
  • Customer

• Not all data is created equally
  • Prioritize data

• Essential to business operation

• Regulated industry information
  • HIPAA

• Data subject to state reporting requirements
BEST PRACTICES PREPARATION

Where Is Your Data Stored?

- Desktop or laptop
- Servers
- Cloud
- Smartphones/Tablets
- Company or personal
- Third parties
BEST PRACTICES PREPARATION

• Who Has Access To Your Data?
  • Employees
  • Drivers
  • Third Parties
• Employee and third party access to data should be controlled
• Data must be protected
  • Educate and train
  • Policies and procedures
BEST PRACTICES PREPARATION

• Destruction of data
  • If you don’t need it, don’t have it
  • Case by case analysis of what data can be destroyed
  • Must consider statutory and regulatory document notification and preservation requirements
  • Litigation considerations

• Statutory considerations
  • State statutes that regulate how and when destroyed
  • Transportation industry specific regulations
BEST PRACTICES PREPARATION

• Steps that you should be taking now
  • Start with your employees
  • Can be your best line of defense
• Educate and train
• Unattended devices in public
• Passwords
• Safeguard sensitive data through encryption
BEST PRACTICES PREPARATION

• Educate on phishing and malware attacks
• Working remotely
• The employee role in responding to a cyber-attack
• Employee education and training
BEST PRACTICES PREPARATION

• Driver shortage and job satisfaction
• Drivers are provided laptops, tablets, and smartphones
• Do employees access network systems remotely?
  • Public Wi-Fi is just that – public
  • There should be no expectation of privacy or security when connected to public Wi-Fi
  • Required to use a VPN connection (Virtual Private Network)
  • The information transmitted via a VPN connection is private and secure and allows an employee to work as if they are directly connected to the network
BEST PRACTICES RESPONDING

Goals For Responding To A Data Breach

- Containment and Recovery
- Evaluation and Response
- Assessment of ongoing Risk
- Notification Requirements
BEST PRACTICES RESPONDING

• Have A “Go To” Team In Place
  • 24 Hour Access
  • The clock starts ticking when the breach occurs
  • Management
  • IT
  • Compliance/HR
  • Attorney
  • 3rd Party/External consultant (Forensics & Media)
• After a breach has occurred is not the time to begin preparing
BEST PRACTICES RESPONDING

• Alert and activate everyone on the response team
  • Management
  • IT
  • Compliance/HR
  • Attorney
  • 3rd Party/External consultant
  • Insurance
  • Media consultant

• Make sure the response team knows their roles and duties and has necessary contact information
BEST PRACTICES RESPONDING

• Secure the premises around the area where the data breach occurred to help preserve evidence
  • “Accident scene” investigation
  • Preservation of information
    • Factual information
    • Equipment
    • Witnesses/participants
  • Control access
BEST PRACTICES RESPONDING

• Stop additional data loss
  • Allow forensics team to analyze
  • Take affected machines offline
  • Do not attempt to analyze yourself
  • Know whether you can or should shut down your system
• Will shutting down system cause loss of information?
• Spoliation issues
BEST PRACTICES RESPONDING

- Document everything about the breach
  - Who discovered it
  - Who reported it
  - To whom it was reported
  - Who knows about it
  - What type of breach occurred
BEST PRACTICES RESPONDING

• Document everything about the breach
  • What was stolen
  • How was it stolen
  • What systems are affected
  • What devices are missing

• Allow counsel to direct the collection of information
BEST PRACTICES RESPONDING

• Assess priorities and risks based on what you know about the breach
• Bring in your forensics firm to begin an in-depth investigation
• Analyze the immediate ramifications of the breach
  • Evaluate and understand the cause of the incident
  • Identify who was affected and what information compromised
BEST PRACTICES RESPONDING

• What is likely to happen to the compromised data
• Are other systems a possible target
• What are the possible legal implications
  • Notification requirements
  • Reporting requirements
  • Litigation risks
BEST PRACTICES RESPONDING

• Identify Legal Obligations
  • Revisit state and federal regulations governing your industry and the type of data lost
  • State or federal law
    • HIPAA, the Fair Credit Reporting Act, etc…
  • Litigation considerations
    • Class action litigation, consumer protection/unfair and deceptive acts, misrepresentation re security of data, negligence, invasion of privacy, breach of express or implied contract, etc…
BEST PRACTICES RESPONDING

• Notify law enforcement
  • After consulting with legal counsel and upper management

• Determine whether law enforcement or other agencies must be notified by law
  • N.C. Gen. Stat. § 75-65
    • Notify the Consumer Protection Division of the Attorney General’s office without unreasonable delay if notice is given to individuals
    • Additional reporting requirements if notice is given to more than 1,000 individuals
BEST PRACTICES RESPONDING

• Continue Working with Forensics
  • Determine if any countermeasures were enabled when the compromise occurred
  • Analyze backup, preserved or reconstructed data sources
  • Begin to align compromised data with customer names and addresses for notification
BEST PRACTICES RESPONDING

• Fix the Issue that Caused the Breach
  • Rely on your forensics team to delete hacker tools
  • Determine if you have other security gaps or risks
  • Put clean machines online in place of affected ones
  • Educate your employees
• Ensure same type of breach will not happen again
  • Passwords
  • Encryption of data
• If it happens once, you are now on notice if it happens again
INSURANCE CONSIDERATIONS

• Cost of responding to a breach increasing
• What is your current insurance coverage
  • Non-cyber policies
    • You may not be covered
• Cyber insurance is changing
  • Exclusions
  • Stand alone policies
INSURANCE CONSIDERATIONS

- Business disruption/lost revenue
- Loss of intellectual property
- Infrastructure damage
- Reputational/brand damage
- Employee concerns
- Regulatory investigations and sanctions
- Litigation exposure
- Remediation and increased protection costs
- Management distraction
- Lower stock price
INSURANCE CONSIDERATIONS

What options are available?

- Buffett style
  - First-party coverage
  - Business interruption
  - Remediation coverage
  - Fines and penalties coverage
  - Risk management services coverage
  - Media relations
  - Extortion
  - Third-party coverage
INSURANCE CONSIDERATIONS

• What should you do?
  • Identify gaps in coverage
  • Work closely with your insurance broker to determine what coverage you have and don’t have
  • Make sure you are aware of changes that are taking place
  • CGL policy may no longer provide protection
  • Determine whether other policies may provide protection
    • E & O policy
    • Officers & Directors policy
CONTRACT CONSIDERATIONS

• Do you share your data?

• With whom do you share your data?
  • Carriers
  • Brokers
  • Customers
  • Third party IT

• What are you sharing?
  • Billing information
  • Social security numbers

• Are these third parties protecting your data?
CONTRACT CONSIDERATIONS

• Contract Considerations
  • Allocation of risk
  • Indemnification
  • Who does data belong to?
  • Who is responsible for the safeguarding data?
  • Cyber security policies and procedures
  • Should be consistent with your standards
  • Access to information
  • Ability to conduct audit of third party’s compliance
  • Insurance
WHAT ELSE CAN YOU DO

• Third Party Forensic Companies
  • “Ethical hacking”
    • Penetration test
      • Proactive attack of network
      • Managed security testing
    • Preventative technology
    • Data loss prevention
  • Data breach response
    • 24 hour response teams
    • Data recovery/remediation
WHAT IS NEXT?

• Internet of Things
• Big Data
• Increased efficiency
  • Interconnectivity
  • Cargo
  • Pallets
  • Fleets
• Example
  • Lights at a terminal monitoring traffic
• Real time analytics
CLOSING THOUGHTS

• Technology continues to evolve
• Everyday we gather more and more data
• If there is money to be made, those seeking to obtain the data will continue to evolve
• You must have an ongoing assessment of technology and data
• What works today may not work tomorrow
• Must adapt to emerging technology and threats
What Data?
I’m A Trucking Company!

Presented by: **Marc C. Tucker**
434 Fayetteville Street, Suite 2800
Raleigh, NC, 27601
919.755.8713
marc.tucker@smithmoorelaw.com

Presented by: **Rob D. Moseley, Jr.**
2 West Washington Street, Suite 1100
Greenville, SC
864. 751-7643
rob.moseley@smithmoorelaw.com