Data Privacy and Cybersecurity

An Overview of the Law for Small and Medium Businesses (SMB)

Presented to the Medford Business Association

By: Robert T. Egan, Esquire

Archer & Greiner, PC

Haddonfield, NJ

November 16, 2016

DISCLAIMER: This presentation is for general information purposes only. It does not constitute legal or tax advice, and may not be used and relied upon as a substitute for legal or tax advice regarding a specific issue or problem. Advice should be obtained from a qualified attorney or tax practitioner licensed to practice in the jurisdiction where that advice is sought.

ARCHER

ATTORNEYS AT LAW

Data Landscape
Trends & Threats

- From 2015 to mid-2016:
  - Estimated 79% of companies experienced cyber incidents
  - 38% Increase in the number of cyber incidents
  - 89% of breaches had a financial or espionage motive
  - Over 50,000,000 people in US received notice of a data breach
  - Organizations are increasing spending on cybersecurity *(http://www.cgma.org/magazine/news/pages/cyber-security-spending-201512001.aspx*).
- 2015 Verizon Study:
  - 2,260 security incidents with confirmed data loss
  - 447 companies with less than 1,000 employees
  - 312 companies with more than 1,000 employees
  - 1501 unknown size

Info Commonly Targeted

- Intellectual Property
- Confidential Information/Trade Secrets
- Money!
- Protected Health Information (PHI)
  - any information about health status, provision of health care, or payment for health care that can be linked to a specific individual
  - includes any part of a patient's medical record or payment history
  - protected under Health Insurance Portability and Accountability Act (HIPAA)

Info Commonly Targeted

- Personally Identifiable Information (PII)
  - a/k/a Sensitive Personal Information (SPI)
  - any information that can be used to distinguish or trace an individual‘s identity
- Examples:
  - Personal identification numbers, including Social Security Number (SSN); driver's license number or State identification card number; financial account number or credit or debit card number; taxpayer identification number; patient identification number
  - Address information, such as street address or email address
  - Names: full name, maiden name, mother‘s maiden name, or alias

Info Commonly Targeted

- More PII Examples:
  - Telephone numbers, including mobile, business, and personal numbers
  - Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)

Info Commonly Targeted

- PII may also include:
  - Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
  - Information identifying personally owned property, such as vehicle registration number or title number and related information
  - Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Source: [NIST, Guide to Protecting Confidentiality of Personally Identifiable Information (PII); Special Publication 800-122, April 2010].

Common Schemes

- Stolen Identity Fraud
  - PII stolen from HR and W-2 (employer or vendor), medical records
  - Phishing
  - Use PII to get: tax refunds; access to bank accounts; access to pre-paid cards; free medical treatment or Rx
- Business E-mail Compromises – Misdirected Money Transfers
  - Hack or spoof home email accounts
  - Target executives, HR or accounting employees
  - Money requests by email or phone

Common Schemes

- Brute force attacks – over 1.4B a day in NJ from various sources worldwide
  - Patches not installed
  - Exploit technical misconfiguration or vulnerability
- Password “acquisition” - >90% of all incidents involve harvesting credentials and using them to log into web applications
- “Malware” - a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

[* Source: 2016 Verizon Data Breach Report]

Malware Types

Virus	A form of malware that relies on human interactions (such as downloading or opening files) to spread.
Trojan	A form of malware that masquerades as a legitimate application.
Worm	A form of malware that can self-replicate and distribute itself across multiple devices without human intervention.
Spyware	A form of malware that discreetly captures and transmits sensitive information from a device (like keystrokes or webcam photos).
Adware	A form of malware whose primary purpose is to serve obtrusive or unexpected ads on the compromised device.
Chargeware	A form of malware that charges the victim money without his/her knowledge or consent.
Ransomeware	A form of malware that restricts access to a device unless the victim pays to have it unlocked.

Common Schemes

- Phishing
  - attempt to obtain sensitive information (e.g., usernames, passwords, credit card details, money) thru an electronic communication
  - “E-mail Spoofing” or “Spearphishing” - pose as trustworthy entity (popular social web sites, auction sites, banks, online payment processors or IT administrators)
    - 30% of recipients click on phishing messages
    - 13% click on attachments
  - IM from anonymous source
  - Links to “malware”

Common Schemes

- Ransomware
  - "Malware" that prevents access to a computer in general or to certain applications or information
    - demand money (a "ransom") to get access
    - threaten to delete vital data or expose other data
  - Sources
    - automatically downloaded from a hacked or compromised malicious website
    - spam emails
    - infected removable drives

Common Schemes

- Mobile Malware
  - Application-Based Threats
    - Privacy threats: gather or use sensitive information (e.g., location, contact lists, personally identifiable information)
    - Vulnerable apps: enable attacker to access sensitive information, perform undesirable actions, or download other apps
  - Web-Based Threats
    - Phishing scams
    - Drive-By Downloads: automatically download an app when you visit a web page
    - Browser exploits: visiting an unsafe web page, can install malware or perform other actions on your device

Common Schemes

- Mobile Malware
  - Network threats
    - from cellular net works as well as local wireless networks (like Wi-Fi or Bluetooth)
    - install malware thru flaws in mobile OS or other software
    - Wi-Fi Sniffing intercepts data traveling between the device and the Wi-Fi access point
- Insider misuse or theft – employees, vendors
- Physical access to systems
- Loss of unsecured devices (laptops and other mobile devices)
- Telework and BYOD vulnerabilities

Costs of Data Breach

- 2016 Ponemon Institute Study: in US, cost was $221 per record
- Up 29% since 2013
- Response costs:
  - Attorneys
  - Forensic Investigation
  - Compulsory Government and Customer Notification
  - Credit Monitoring & ID Theft Insurance
- Liability to victims
- Loss of sales – website shutdown or reduced traffic

Costs of Data Breach

- Business Interruption
  - Staff hours
  - Diversion of staff resources
  - "Reputation" Damage
    - loss of goodwill
    - devaluation of trade name
    - customer "churn"
- IP – *e.g.,* plans, designs, R&D become public
- Increased cost to raise debt
- Insurance premium increases
- Legal fees and expenses

Legal Landscape
Federal

- Federal Trade Commission Act *(obtaining and/or failure to protect consumer information may be a deceptive/unfair trade practice; several administrative rules for targeted industries; many enforcement actions)*
- Children's Online Privacy Protection Act (COPPA) *(unfair/deceptive practices related to children <13)*
- Consumer Financial Protection Bureau
- Fair Credit Reporting Act (FCRA)
- Fair and Accurate Credit Transactions Act of 2003
- SEC Disclosure Guidance (Sarbanes-Oxley, Dodd-Frank)
- Gramm-Leach-Bliley Act (GLBA) *(financial services; nonpublic personal information, "NPI")*

Legal Landscape
Federal

- HIPAA *(protected health information, "PHI")*
- Electronic Communications Privacy Act (ECPA) *(Customer Proprietary Network Information, "CPNI")*
- Cybersecurity Information Sharing Act of 2015 (CISA)
- Family Educational Rights and Privacy Act (FERPA) *(privacy of student education records)*
- Government Procurement Requirements, including DoD Regulations *(applicable to private contractors, imposing broad cyber incident reporting requirements, 32 C.F.R. part 236)*
- IRS Regulations
- Computer Fraud & Abuse Act
- Various Executive Orders

Legal Landscape
State Law Requirements

- State Data Breach Notification Laws in 47 states
  - Generally, require notice to victims and authorities of a "data breach"
  - Different scope from state to state
  - Usually depends upon where the "customer" is
  - Different definitions of "breach"
    - NJ and some others: unauthorized ***access*** to ***unencrypted*** personal information constitutes a breach, even absent evidence that the personal information accessed was actually acquired or taken
    - Ransomware attack may require notice even if no data copied or stolen
  - Different definitions of "personal information"
  - Different notice requirements

Legal Landscape

State Law Requirements

New Jersey

- NJSA 56:8-161 *et seq (*"Identity Theft Prevention Act")
  - Requires notice of data breach in many circumstances
    - State Police
    - Customers
  - Once PII is no longer to be retained, must shred, erase or otherwise modify "to make it unreadable, undecipherable or nonreconstructable through generally available means."
  - SSN restrictions - cannot post, publicly display, make available to the general public, print under certain circumstances (or do a few other things)
  - Statute not applicable if PII data was encrypted or secured by any other method or technology that renders it unreadable or unusable
  - Might be liable to customer for 3X damages and attorneys fees if you fail to comply with notice or SSN requirements
    - For example, failure to give notice of data breach causes customer to delay addressing ID theft, causing additional "loss"
  - NJ government can enforce and impose penalties

Legal Landscape
State Law Requirements

- State Data Security Standards
  - Affirmative duties to do things to protect info over and above notice requirements in Massachusetts, California and Nevada
  - May apply if you have information from a person who resides in one of these states
- Duty to provide security is expanding
  - Some states impose responsibility for failure to take reasonable measures to keep PII confidential in certain circumstances even if there is no statute or regulation
  - FTC has taken aggressive stance against "big" companies with "big" breaches https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises

Small and Medium Businesses

<u>Small and midsized operations</u>

Same threats + fewer resources = easier target

Small and Medium Businesses

- Small businesses are unsuspecting targets
  - Believe they do not have anything worth stealing
  - Do not “get” risks of attack or costs of data breach
  - Do not have IT budgets, risk management mentalities or adequate security training
  - 62% of cyberattacks are against small and medium businesses
    - Average cost per event = $188,242
    - 60% out of business in a year

Small and Medium Businesses

- Small businesses typically have:
  - Employee (e.g., SSNs, health info) and customer data (e.g., credit card #s)
  - Bank account information and access to the business's finances
  - Intellectual property/confidential information
  - Access to larger networks such as supply chains
  - Hackable websites

SMB – What Law Applies to Me?
Specific Regulated Industries

- Lending/Financial Services/Banking
- Collections
- Securities
- Publicly Traded
- Health Care
- Higher Education
- Government Contractors
- Communications Common Carriers
- Automakers and their Suppliers
- Medical Device Makers
- Insurance

SMB – What Law Applies to Me?
Everyone (or Almost Everyone)

- Data Breach Notification Laws
- Certain state laws that require you to take security measures for PII
  - Broad requirements if you have a location in CA, NV or MA
  - Specific, less comprehensive requirements in other states

SMB – What MUST I Do?

- If in a regulated industry, consult an attorney regarding specific requirements
- Consult an attorney ASAP if you think you've been hacked!
- Give "notice" of unauthorized access, acquisition or use of PII or PHI if the law or a contract requires it, or you risk:
  - Liability to victims (up to triple damages + attorneys' fees in NJ)
  - Fines
  - Loss of (more) customers/sales
- In NJ:
  - When you discard PII, shred, erase or otherwise modify it "to make it unreadable, undecipherable or nonreconstructable"
  - Do not "disclose" SSNs to unauthorized persons

SMB – What Should I Do?

- Employ basic best practices*
  - Minimize collection, use and storage of PII, PHI and your trade secrets and confidential info
  - Encrypt
  - "Shred" old information (digitally or in hard copy)
  - Redact, limit or eliminate use of SSN
  - Do not store credit card numbers
    - Understand and comply with the Payment Card Industry Data Security Standard (PCI DSS) - applies to all entities that store, process or transmit cardholder data**
    - If you must store, store only last four digits and/or encrypt

* See *e.g.*, *https://oag.ca.gov/cybersecurity*; *https://www.fcc.gov/general/cybersecurity-small-business*; *https://www.identitytheft.gov*;)

** https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

SMB – What Should I Do?

- Employ basic best practices*
  - Limit user access to "need to know"
  - Protect your network
    - Technically (e.g., server splits, firewalls, patches, upgrades, security tools, restrict computer ports)
    - Operations (e.g., email policies, password policies)
  - Talk to a data security professional if you need help with these basics

* See *e.g.*, *https://oag.ca.gov/cybersecurity*; *https://www.fcc.gov/general/cybersecurity-small-business*; *https://www.identitytheft.gov*;)

SMB – What Should I Do?

A Few Basic Best Technical Practices

- Use different passwords for personal and business
- Use complex or cognitive passwords
  - Complex – “B3%nT92”
  - Cognitive
    - a sentence followed by something that changes
    - Example: I’mEasilyConfused$[add something for each site/app/system]
- Consider “multifactor authentication”
- Do not attach thumb drives to your computer unless you are sure of the source!
- Be vigilant about emails asking for anything unusual or suspicious or confidential – send money to any one, financial information

SMB – What Should I Do?

- Talk to your insurance agent/broker (and perhaps an attorney) about cyber insurance
- Enforce your cyber security policies and procedures
  - Don't assume compliance
  - Inspect what you expect
- Watch your contracts with others, including vendors, consultants, contractors and employees
  - Any contract that affects "data" or sensitive information, for example:
    - Payroll companies
    - Accounting firms
    - Supply chains
  - You may want to impose duties on those to whom you make disclosures
  - Vendors may impose duties on you

SMB – What Should I Do?

- Consider retaining an attorney to:
  - Draft/edit contracts that affect "data":
    - Ownership/licensing of data
    - Define personal information and highlight sensitive information
    - Minimum security safeguards
    - Oversight of security compliance (customer audits, auditing by service provider, security questionnaire)
    - Notice/disclosure of security breaches or privacy-related compliance issues
    - Security breach procedures or cooperation (timing, method of contact)
    - Expenses of breach remediation
    - Return/destruction of personal information

SMB – What Should I Do?

- Consider retaining an attorney to:
  - Review/write employee policies regarding:
    - email and privacy policies
    - codes of conduct
    - password
    - BYOD (bring your own device)
    - social media
    - other cyber-related issues
    - trade secrets, confidential information and intellectual property
  - Discuss whether to retain data security professionals
  - Not a one-size fits all situation
    - Threat assessment
    - Costs and resources

SMB – What Should I Do?

- Consider retaining a data security professional to:
  - Conduct a cybersecurity assessment
  - Help develop an incident response plan and team:
    - Attorney
    - Management
    - Inside technical experts
    - Outside technical experts (investigation and remediation)
    - HR
    - PR (optional)
  - Practice your incident response plan
  - Test the effectiveness of your security measures
  - Not a one-size fits all situation
    - Threat assessment
    - Costs and resources

Data Privacy & Cybersecurity
Additional Resources for NJ Businesses

- Identity Theft
  - Prevention - Consumer Reports, Nov. 2016, at 28-37
  - Response - https://www.identitytheft.gov/
- Data Breach
  - Prevention - https://www.ftc.gov/datasecurity
  - Prevention - https://www.cyber.nj.gov/
  - Response - https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf
  - Response - https://www.cyber.nj.gov/data-breach-notifications

Follow Up Questions?

Feel Free to call me at

856-354-3079

ARCHER

ATTORNEYS AT LAW