CYBERSECURITY TRENDS & EMERGING ISSUES

ABOUT BECKAGE

- Law firm focused on technology and data security and privacy.
- Beckage firm includes Certified Information Privacy Professionals by the International Association of Privacy Professionals (IAPP), IT professionals, former tech entrepreneurs, federal regulator, former Chief Information Security Officer (CISO), business owners and former public-company executive.
  - **Regulatory Compliance** – Policy drafting, contract review, training and tabletop exercises.
  - **Incident Response** – Help mitigate legal risk in breach response and identify and coordinate legal notifications and reporting obligations.
  - **Litigation** – Represent clients in federal and state technology, data breach and privacy litigations, and during audits and investigations.
  - **Risk Management** – Work with clients to evaluate IT network and enterprise from a legal and risk management perspective with Beckage's internal Certified Information Systems Auditor (CISA).
- Beckage is proud to be a certified Women-Owned Business Enterprise (WBE).

JENNIFER A. BECKAGE, ESQ. CIPP/US, CIPP/E

Email: jbeckage@beckage.com
Cell: (716) 510-0306

- *Certified Information Privacy Professional, United States (CIPP/US) and Certified Information Privacy Professional, Europe (CIPP/E) as certified by the International Association of Privacy Professionals (IAPP)*
- *Recognized in 2018, 2019, and 2020 as one of the Top 30 data breach attorneys in the United States by Cybersecurity Docket*
- *Upstate New York Super Lawyers® Super Lawyer 2019 and 2020, only attorney recognized within Technology Transactions category*
- *Developed multiple privacy and security programs*
- *Responded to numerous data security incidents, cyberattacks, ransomware, malware by providing legal and risk mitigation advice while coordinating appropriate technical and other teams to respond and stand up operations again*
- *Represented clients in federal and state data breach and privacy litigation, including defending clients in putative class actions*
- *Former tech business owner; sold company to publicly-traded company and retained as VP Operations of technology products*

PRESENTATION OVERVIEW

- **Legal Landscape – Privacy v. Security**
- **Legal Landscape – Data Security**
  - States – NY SHIELD Act
- **Cybersecurity Threat Landscape**
  - Phishing/Spearphishing/Vishing
  - Ransomware/Malware
- **Ethical Obligations to Safeguard Client Data**
- **Best Practices (in the office and remotely)**

LEGAL LANDSCAPE – PRIVACY V. SECURITY

- **Privacy**
  - Leave me alone/let me control processing of my data.
- **Security**
  - Keep information safe from unauthorized users.

LEGAL LANDSCAPE – DATA SECURITY

- **Data Security**

LEGAL LANDSCAPE – DATA SECURITY

- Data Security
  - Federal statutes – GLBA, HIPAA, etc.
  - All 50 states have data breach laws.
  - Now states are adding data security requirements into their laws.
  - New York:
    - DFS Cybersecurity Regulation (22 NYCRR 500).
    - "Stop Hacks and Improve Electronic Data Security" (SHIELD) Act, which broadens New York's data breach notification law and imposes data security requirements.
      - No private right of action but does authorize civil penalties by the AG.
      - Deadlines: Breach notification requirements were effective October 23, 2019 and compliance with the data protection requirements was due March 21, 2020.

LEGAL LANDSCAPE – DATA SECURITY

- "Private information" includes information concerning a natural person plus:
  - Social Security number;
  - Driver's license number or non-driver ID card number;
  - Account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;
  - Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password;
  - Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or
  - A username or email address in combination with a password or security question and answer that would permit access to an online account.

LEGAL LANDSCAPE – DATA SECURITY

- "Reasonable Security" Requirement: remember your A, T and P.
  - A business will be deemed to be in compliance if it is a "compliant regulated entity" or implements a "data security program" that includes the following reasonable safeguards:
  - **Reasonable administrative safeguards** such as the following, in which the person or business:
  - designates one or more employees to coordinate the security program;
    - identifies reasonably foreseeable internal and external risks;
    - assesses the sufficiency of safeguards in place to control the identified risks;
    - trains and manages employees in the security program practices and procedures;
    - selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and
    - adjusts the security program considering business changes or new circumstances.

LEGAL LANDSCAPE – DATA SECURITY

- **Reasonable technical safeguards** such as the following, in which the person or business:
  - assesses risks in network and software design;
  - assesses risks in information processing, transmission, and storage;
  - detects, prevents, and responds to attacks or system failures; and
  - regularly tests and monitors the effectiveness of key controls, systems, and procedures.
- **Reasonable physical safeguards** such as the following, in which the person or business:
  - assesses risks of information storage and disposal;
  - detects, prevents, and responds to intrusions;
  - protects against unauthorized access to or use of private information during or after the collection, transportation, and destruction or disposal of the information; and
  - disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

LEGAL LANDSCAPE – DATA SECURITY

- Breach Notification Requirement:
  - The SHIELD Act broadens the definition of what constitutes a "breach" to include not just acquisition of private information, but also access to such private information.
  - There is an exception for inadvertent disclosures of private information by authorized persons that are not likely to result in misuse of information, financial harm, or emotional harm.
    - If applicable, document such determination.

LEGAL LANDSCAPE – DATA SECURITY

- Small businesses are subject to the reasonable safeguards requirement, however the SHIELD Act allows that safeguards may be "appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."
  - A small business is defined as one with fewer than fifty employees, less than $3 million in gross annual revenue in each of the last 3 years, or less than $5 million in year-end total assets.
- For reasonable safeguard requirement violations, the court may impose penalties of not more than $5,000 per violation.

LEGAL LANDSCAPE – DATA SECURITY

- Besides New York's SHIELD Act, many other states have data security provisions in their data breach notification laws.
- Also, data security requirements are starting to sneak into data privacy laws; e.g., the California Consumer Privacy Act (CCPA) references Cal. Civil Code requiring reasonable security safeguards.

CYBERSECURITY THREAT LANDSCAPE

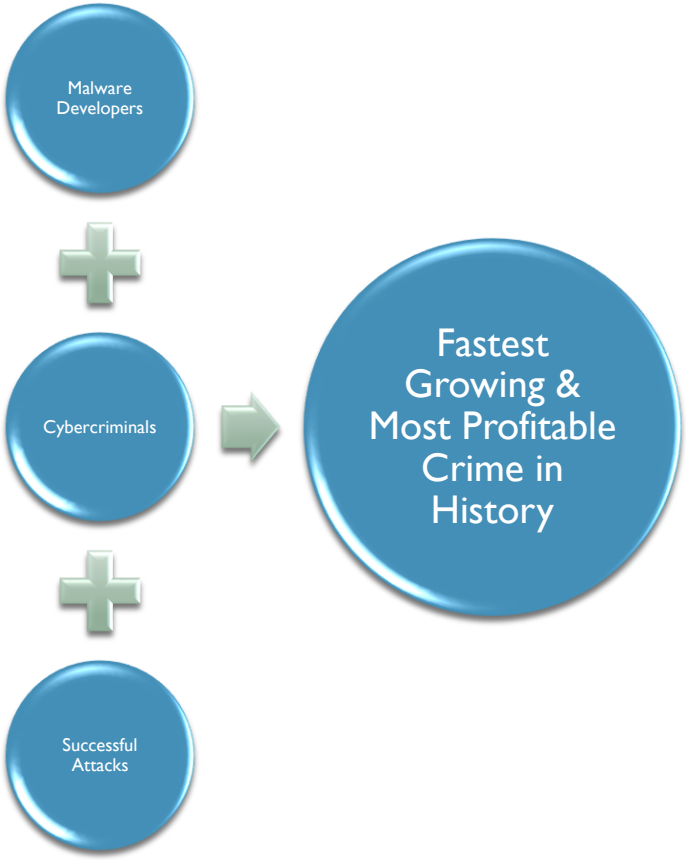
CYBERSECURITY THREAT LANDSCAPE – SOCIAL ENGINEERING

- The use of confidential data to perpetrate fraud or blackmail.
- Inadvertent disclosure of confidential data by careless employees.
- Theft of company trade secrets.
- Disclosure of confidential information by disgruntled or former employees for financial gain.

CYBERSECURITY THREAT LANDSCAPE – PHISHING & SPEARFISHING

- **Overview:** fraudulent emails that attempt to steal your data.
- **Examples:**
  - Asking you to confirm your account.
  - Asking you for login information or passwords.
  - Asking you to click on links (that contain malware that is downloaded onto your systems).
- **Things to watch for:**
  - Check the sender's email address.
  - Review whether it appears to come from a high-level employee (Managing Partner).
  - Do not click on unverified links.

CBERSECURITY THREAT LANDSCAPE – RANSOMWARE/MALWARE



Statistics

- North American threat detections saw a 10% increase in 2019 over 2018.
- The average cost of a ransomware attack on businesses is $133,000.
- Businesses fell victim to a ransomware attack every 14 seconds in 2019 with an estimation of every 11 seconds by 2021.
- PII accounted for 98% of all data breached in 2019.

https://resources.malwarebytes.com

ETHICAL OBLIGATIONS TO SAFEGUARD YOUR CLIENT'S DATA

- All industries face challenges related to data security and privacy and keeping information confidential.
- Organizations face a number of laws and regulations and industry standards that may be applicable to them.
- Lawyers are faced with ethical rules that guide handling of client information – tangible and electronic.

ETHICAL RULES

- Competence – Rule 1.1
- Duty of Confidentiality – Rule 1.6
- Supervising Non-Lawyers or Subordinate Lawyers – Rule 5.3

ETHICAL RULES – RULE 1.1

- Rule 1.1, comment 8(ii): As of March 28, 2015, lawyers must keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients to store or transmit confidential information.

ETHICAL RULES – RULE 1.1 (CONT'D)

- Ethics rules require lawyers to have technological competence.
- Understand technology used to protect firm data and client data.
- Understand electronic discovery rules in the relevant jurisdictions.
- Use available technology to guard against foreseeable attempts to infiltrate data.
- Investigate vendor security practices and periodically review to be sure they remain up-to-date.
- Investigate any potential security breaches or lapses by vendor to ensure client data was not compromised.

ETHICAL RULES – RULE 1.6

- Rule 1.6 Confidentiality of Information
  - Rule 1.6(a): A lawyer shall not knowingly reveal confidential information (unless there is consent or authorization to do so as set forth in the Rule).
  - Rule 1.6(c): A lawyer shall make **reasonable efforts** to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

ETHICAL RULES – RULE 1.6 (CONT'D)

- Rule 1.6, comment 16: Paragraph (c) imposes three related obligations. It requires a lawyer to make reasonable efforts to safeguard confidential information against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are otherwise subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3.
- Rule 1.6, comment 16: Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or software excessively difficult to use).

ETHICAL RULES – RULE 1.6 (CONT'D)

- The ethical rules require lawyers to take reasonable steps to safeguard the confidentiality of client data.
- Just like with paper files, lawyers must work to protect the intangible, electronically stored information (ESI) in their possession.
- Lawyers must take steps to safeguard confidential information against their own inadvertent disclosures and those of others participating in the representation AND act competently to safeguard confidential information against unauthorized access by third parties.

ETHICAL RULES – RULE 1.6 (CONT'D)

- Lawyers must assess whether circumstances warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

ETHICAL RULES – RULE 5.3

- Rule 5.3 Responsibility Over Non-Lawyers
  - Rule 5.3(b): A lawyer is responsible for certain conduct of a non-lawyer employed or retained by or associated with the lawyer.

ETHICAL RULES – RULE 5.3 (CONT'D)

- Rule 5.3, comment 3: A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. One such example is using an Internet-based service to store client information. When using outside services, the lawyer must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer and law firm. The extent of reasonable efforts required under this Rule will depend upon the circumstances, including: (a) the education, experience, and reputation of the nonlawyer; (b) the nature of the services involved; (c) the terms of any arrangements concerning the protection of client information; (d) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality; (e) the sensitivity of the particular kind of confidential information at issue; and (f) whether the client will be supervising all or part of the nonlawyer's work. When retaining or directing a nonlawyer outside the firm, a lawyer should appropriately communicate directions to give reasonable assurance that the nonlawyer's conduct is compatible with the lawyer's professional obligations.

ETHICAL RULES – RULE 5.3 (CONT'D)

- How to supervise nonlawyers on technology matters.
  - Rule 1.1, cannot simply delegate or outsource competence.
- Keep in mind obligations to help ensure that internal and external nonlawyer assistants carry out their duties in a manner that is compatible with the lawyer's professional obligations.

ETHICS – SOME KEY DECISIONS

- Backups and Record Retention
  - N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 940 (2012). "A lawyer may use off-site backup tapes to store confidential client information if the lawyer takes reasonable care to ensure that the storage system, and the arrangements for its use, adequately protect the confidentiality of such information." See also, N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 842 (2010) (same principles addressed in determining reasonableness and use of cloud storage); N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 1020 (2014). Authorized persons should have access to cloud storage containing confidential information.

ETHICS – SOME KEY DECISIONS

- N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 842 (2010). Addresses Rule 1.6 and reiterates that an attorney must take reasonable steps to protect confidential information. Reasonable care may include consideration of the following:
  - that there is a way to ensure that the provider has enforceable obligations to preserve confidential information;
  - that there is a method by which to investigate providers' security measures;
  - that the provider employs technology to guard against access to data; and
  - that the provider has the ability to wipe data/move it. See, N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 1020 (2014).

ETHICS – SOME KEY DECISIONS

- N.Y. St. Bar Ass'n Comm. on Prof. Ethics Op. 1019 (2014). In providing lawyers remote access to client files, a law firm must take reasonable steps to protect information, but: "Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients."
- N.Y. St. Bar Ass'n Comm. on Prof. Ethics Formal Op. 2017-5 (2017). During border searches, confidential information may be on the attorney's electronic devices, which may be searched.
- N.Y. St. Bar Ass'n Comm on Prof. Ethics Op 749 (2001). A lawyer may not ethically use technology to surreptitiously examine and trace email and other electronic documents; e.g., placing a "bug" in an email that the lawyer sends to determine the subsequent route of the email.

BEST PRACTICES

1. Practice Good Password Hygiene
2. Monitor Emails
3. Transmit Data Securely
4. Destroy Data Securely
5. Report Incidents!

BEST PRACTICES: REMOTE WORKING

1

Secure your home workspace

2

Avoid posting pictures of your workspace

3

Use a personal hotspot or encrypt home wireless networks

QUESTIONS?

Beckage
Legally Focused. Technology Driven.

WE ARE LAWYERS, SO WE HAVE A LEGAL DISCLAIMER

- Thank you.
- The information is not legal advice for any specific matter as each matter should be evaluated on a case-by-case basis. The recipient of this publication cannot rely on its contents.
- If legal advice is required for any specific matter, please contact an attorney at Beckage or visit Beckage.com.
- Follow us on LinkedIn.
- Visit our blog for timely articles and subscribe for blog articles and newsletter: Beckage.com/blog.