Data Security 101
A Lawyer's Guide to Ethical Issues in the Digital Age

CLARK HILL

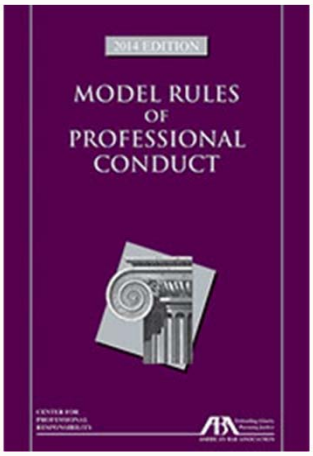
Christopher M. Brubaker
cbrubaker@clarkhill.com
Pennsylvania Bar Institute, Business Lawyers' Institute
11.7.18

ABC's of Cyber Risk

- Types of Risk
- Ethical Obligations
- Reasonable Measures
- Risk management is critical to Cyber Risk
- Cyber Risk is still an emerging market in the insurance industry
  - Risks, coverages and controls are all evolving
  - Underwriting involves risk management assessment
- Statutory and Regulatory Requirements

Rules to Live by

Rule 1.0 (“Terminology”)
Rule 1.1 (“Competence”) Rule 1.4 (“Communication”) Rule 1.6 (“Confidentiality of Information”)
Rule 1.15 (“Safekeeping Property”)
Rule 5.3 (“Responsibilities Regarding Nonlawyer Assistants”)



Cyber Threats

- Hacking
  - Direct attack on computer network or information systems
  - Can come from external and internal sources
  - Can be simply mischievous or part of an organized attack on the system as a whole
  - Utilize a variety of techniques – phishing, social engineering, watering hole

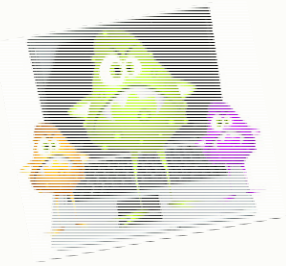
Types of Cyber Risk

- Data Breach/Loss
  - Client confidential information (Personal/Medical/Financial)
  - Confidential or proprietary information (Trade Secrets)
  - Business Plans
  - Internal communications
- Denial of Service

CLARK HILL

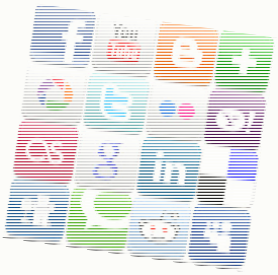
Types of Cyber Risk

- Damage to electronic infrastructure
- Malware/virus
  - Traditional virus that corrupts data/makes system unusable
  - Malicious code used as part of a larger scheme to steal data
  - Cyber Extortion
- Use/misuse of social media and the internet
  - Defamation (libel/slander)
  - Trademark infringement



CLARK HILL

Cyber Threats



- Employees and Other Insiders
  - Disgruntled Employee
  - Malicious Employee
  - Untrained/Careless
  - Activist (Snowden/Manning)
  - Unauthorized Access, Use or Connectivity
    - Surfing the web and playing games
    - Hooking up personal devices to the system

CLARK HILL

Statistics on Insider Threats

2013 survey (IT security professionals):

41% viewed rogue employees as the biggest threats to their organizations*

2013 report:

54% of IT security professionals believe that insider threats are more difficult to detect/prevent today than in 2011**

FBI Chief Information Security Officer: 2013:

25% of the incidents in its networks are from "knucklehead" problems***

* Avetco Press Release (June 7, 2013) www.avecto.com/news-events/press-releases/80-of-it-security-professionals-say-their-greatest-threats-are-from-rogue-employees,-malware-exploits-or-unauthorized-software

** Vormetric Insider Threat Report (October 2013) http://enterprise-encryption.vormetric.com/analyst-report-esg-insider-threat.html

*** Information Week Dark Reading (March 1, 2013) http://www.darkreading.com/vulnerabilities---threats/5-lessons-from-the-fbi-insider-threat-program/d/d-id/1139281?

CLARK HILL

Summary of Insider Threat Reports by Mariana Noll on IT Security Central, April 3, 2018

Netwrix 2018 Cloud Security Report

- Almost 58% of organizations that had security incidents over 2017 blamed them on insiders.
- 45% respondents, whether or not they experienced a security incident, still see their own employees as the biggest threat to security.

Kaspersky – The Human Factor in IT Security

- 52% of businesses admit that employees are their biggest weakness in IT security.
- Most worry about employees sharing inappropriate data via mobile devices (47%), the physical loss of mobile devices exposing their company to risk (46%) and the use of inappropriate IT resources by employees (44%).
- In 46% of cyber security incidents in the last year, careless or uninformed staff have contributed to the attack.
- Employee carelessness contributed directly to 48% of cyber security incidents, accounting for even more incidents than the theft of devices, which only contributed towards a third (37%) of incidents.

Cisco 2018 Annual Cyber Security Report

- According to security professional respondents:
- The most challenging areas and functions to defend are mobile devices, data in the public cloud, and user behavior.

PwC – US State of Cybercrime Survey

- 44% of data breaches are attributable to insiders.
- 90% of insiders displayed no worrying characteristics prior to their attacks.
- 80% of attacks are committed during work hours on company issued software.

Hiscox Cyber Readiness Report 2018

- 73% of studied organizations fell into the novice category, suggesting they have some way to go before they are cyber-ready.
- 57% of the organizations surveyed claim to be 'very confident' in their cyber security readiness.

Cyber Threats

- Mobile Devices
  - **Lost, misplaced or stolen**
  - Weak or no user authentication
  - Intercepted wireless
  - Malware/Malicious attachments
  - Malicious or compromised websites
  - Phishing
  - Shortened URLs
  - QR Codes

Ethical Obligations

- Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200 ("Opinion 2011-200")
- Duty to Safeguard Rule 1.15
  - Affirmative duty to safe keep client property
  - Applies to records and files
- Duty to Keep Up with Technology Rule 1.1
  - "Competence" includes adopting technological advancements in the practice of law
  - Need to stay current with changes in technology and how they impact the profession

Ethical Obligations

- "Informed Consent" defined in Rule 1.0
- Client Confidentiality Rule 1.6
  - Affirmative duty to keep client data secret
  - Affirmative duty to protect data
  - Client can give informed consent to disclosure and means of safeguarding data
- Need to keep clients informed Rule 1.4
- Obligation to supervise non-attorneys Rule 5.3
  - Extends to third-party service providers
  - May implicate laws in other countries

Reasonable Measures

The Explanatory Comments to Rule 1.6 provide guidance on how to assess whether conduct is reasonable. Comment 25 addressing safeguarding client information provides in part:

> Factors include, but are not limited to,
>
> the sensitivity of the information,
>
> the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards,
>
> the difficulty of implementing the safeguards, and
>
> the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

More on Reasonable Measures

Rule 1.6, Explanatory Comment 25 continued:

> A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.
>
> Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as laws that govern data privacy or that impose notification requirements is beyond the scope of these Rules.

Comment 26 addressing communications is structured the same

ABA Formal Opinion 477R – May 22, 2017

- Securing Communication of Protected Client Information
  1. Understand the nature of the threat;
  2. Understand how client confidential information is transmitted and where it is stored;
  3. Understand and use reasonable electronic security measures;
  4. Determine how electronic communications about client matters should be protected;
  5. Label client confidential information;
  6. Train lawyers and nonlawyer assistants in technology and information security; and,
  7. Conduct due diligence on vendors providing communication technology.

Data Security Basics

- Cybersecurity is based on a risk management approach
- There is no set answer or approach – what is right for Mega Firm is not the same for solo or small firm
- Technology is not the (only) answer
- Requires constant attention and adaptation
- Attorneys should aim high and seek to be at the head of the class when it comes to cybersecurity
- Develop a formal cybersecurity plan including what to do in the event of a breach
- Train employees on cybersecurity basics including passwords, encryption and how to spot suspicious email

Risk Management Approach to Cybersecurity

Risk Management Techniques

- Security Assessment – what info do you have, how is it used, what security features are in place? Select safeguards to fit your specific needs
- Information Security Policies – address all types of information assets
  - Written Records Management - document classification, protection & destruction protocols
  - Business Continuity and Incident Response Plans
  - Confidentiality Agreements – employees, vendors & contractors
  - Employee Usage – internet, email, devices, passwords
- Security: Premises, Web Server, Mobile Device, Service Providers
  - Utilize technology – firewalls, encryption, virus prevention, system monitoring, etc.
  - Protect All Electronic Media: laptops, smartphones, tablets, backup tapes, CDs, USB drives
  - Backup & Archive
- Monitor, monitor, monitor

ABA Formal Opinion 483 – October 17, 2018

Lawyers' Obligations after an Electronic Data Breach or Cyberattack

- Based on obligations in Rules 1.1, 5.1, and 5.3 "lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services related to data and the use of data."
- When a breach of client information is detected or suspected a lawyer must act reasonably and promptly to stop the breach and mitigate damage caused by the breach.
- Must notify current clients of data breach
- Compliance with applicable breach notification laws

Common Law and Contractual Obligations

- Competence and diligence
- Confidentiality
- Keep client reasonably informed & communicate

Restatement (Third) Of The Law Governing Lawyers §16 (2000)

Contractual duties and obligations – what did you agree to in the retainer agreement

Statutory and Regulatory Duties - Federal

- Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Requires certain financial institutions as well as health care providers, or businesses that provide services to health care providers, notify patients and the government if the security of the personal information they maintain is breached
  - Minimum Security Standards

Statutory and Regulatory Duties - State

- No uniform federal data breach notification law
  - State laws control and often conflict
- ~~Nearly~~ every state, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, has enacted legislation requiring notification of security breaches involving personal information
  - ~~Exceptions: Alabama, New Mexico, and South Dakota~~

Wrap-Up

- Attorneys have ethical obligation to safeguard client information and communications
- Attorneys have ethical obligation to keep abreast of developments (technology) that improve the delivery of legal services to clients
- Attorneys may be subject to additional requirements under law or by contract
- Effective cybersecurity requires constant monitoring and adaptation
- Questions

CLARK HILL

Christopher M. Brubaker

cbrubaker@clarkhill.com
215.640.8516

One Commerce Square
2005 Market Street, Suite 1000
Philadelphia, PA 19103

THIS COPYRIGHTED MATERIAL IS PROTECTED BY THE COPYRIGHT LAWS

CLARK HILL