PROGRAM MATERIALS
Program #3090
May 28, 2020

Digital Risks and Digital Duties: Finding a Standard of Care in Cyberspace – Part 1

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Digital Risks and Digital Duties: Finding a Standard of Care in Cyberspace

James M. Paulino, II, Esq., CIPP/US
585.295.8351 | jpaulino@goldbergsegalla.com

Michael A. Goode, Esq., CIPP/US
919.582.0819 | mgoode@goldbergsegalla.com

GOLDBERG SEGALLA

Do the best you can until you know better. Then when you know better, do better.

Maya Angelou

GOLDBERG SEGALLA

Overview

1. What's the Harm?
2. Liability Triggers
3. Risks
    a. Bad People
    b. Bad Technology
    c. Bad Education
4. Reasonableness Guideposts
    a. Statutory Requirements
    b. Industry Requirements
    c. Experts
5. Examples and Explanations
6. Best Practices Roundup

GOLDBERG SEGALLA

What's the Harm?

1. Human Rights Violations
    a. GDPR / CCPA
2. Crown Jewels
3. Long Arm of the Law
4. Public / Shareholder Opinion

What's the Harm?

Human Rights: GDPR

Art. 1 Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects **fundamental rights and freedoms of natural persons** and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

What's the Harm?

Human Rights: CCPA

1798.100: right to request disclosure of the categories and specific pieces of personal information the business has collected

1798.105: right to request deletion of any personal information about the consumer which the business has collected from the consumer

1798.110: right to request disclosure of data information, including sources, pieces of data, and company purposes for using data.

1798.115: right to request seller of data to disclose data and practices information.

1798.120: right to "opt-out" (direct businesses not to sell consumer information).

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]
(Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)

Illinois Biometric Information Privacy Act

Sec. 5. Legislative findings; intent. The General Assembly finds all of the following:

(c) **Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse**, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

Ill. Comp. Stat. Ann. 14/5 | P.A. 95-994, § 5, eff. Oct. 3, 2008.

Liability Triggers

1. Common Law
2. Shareholders
3. Governmental
4. Statutory
5. Contract

Liability Triggers

Common Law / Negligence

Most courts apply a reasonableness negligence-type standard when dealing with data breach claims related to consumer information entrusted to a commercial entity.

See In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014), order corrected, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

Liability Triggers

Common Law / Negligence

Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. *See, e.g., Witriol v. LexisNexis Grp.*, No. C05–02392 MJJ, 2006 WL 4725713, at *8 (N.D.Cal. Feb. 10, 2006); *CUMIS Ins. Soc'y., Inc. v. BJ's Wholesale Club, Inc.*, No. 051158, 2005 WL 6075375, at *4 (Mass.Super.Dec. 7, 2005) *aff'd*, 455 Mass. 458, 918 N.E.2d 36 (2009); *Yakubowicz v. Paramount Pictures Corp.*, 404 Mass. 624, 536 N.E.2d 1067, 1070 (1989) ("A basic principle of negligence law is that ordinarily everyone has a duty to refrain from affirmative acts that unreasonably expose others to a risk of harm."). As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of **industry-standard** encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach.

See In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014), order corrected, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

Liability Triggers

Common Law / Fiduciary Duty

This case implicates the "failure-to-monitor" theory of director liability first articulated by the Delaware Court of Chancery in *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996). "*Caremark* claims inevitably arise in the midst of or directly following 'corporate trauma' of some sort or another," and are premised on directors' conscious failure to monitor corporate action, thereby "breaching their fiduciary duties in bad faith in a manner that caused the corporate trauma." *Horman v. Abney*, C.A. No. 12290-VCS, 2017 WL 242571, at *5 (Del. Ch. Jan. 19, 2017). Here, Plaintiff alleges that Rowlands breached her *Caremark* duties by failing to monitor USIS's cybersecurity practices despite the known risk of a cyberattack. This dereliction, according to Plaintiff, permitted a massive cyber-intrusion to go undetected for months, and eventually led to USIS's bankruptcy after its largest client revoked multi-billion dollar contracts in response to the security breach.

Corp. Risk Holdings LLC v. Rowlands, No. 17-CV-5225(RJS), 2018 WL 9517195, at *3 (S.D.N.Y. Sept. 28, 2018)

Liability Triggers

Shareholder Claims:15 U.S.C.A. § 78u-4

(b) Requirements for securities fraud actions

(1) Misleading statements and omissions In any private action arising under this chapter in which the plaintiff alleges that the defendant—

(A) made an untrue statement of a material fact; or

(B) omitted to state a material fact necessary in order to make the statements made, in the light of the circumstances in which they were made, not misleading;

the complaint shall specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed.

Liability Triggers

State Law Claims

Massachusetts Consumer Protection Act

In re Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1338 (N.D. Ga. 2019)

(a) Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.

(b) It is the intent of the legislature that in construing paragraph (a) of this section in actions brought under sections four, nine and eleven, the courts will be guided by the interpretations given by the Federal Trade Commission and the Federal Courts to section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)), as from time to time amended.

(c) The attorney general may make rules and regulations interpreting the provisions of subsection 2(a) of this chapter. Such rules and regulations shall not be inconsistent with the rules, regulations and decisions of the Federal Trade Commission and the Federal Courts interpreting the provisions of 15 U.S.C. 45(a)(1) (The Federal Trade Commission Act), as from time to time amended.

Mass. Gen. Laws Ann. ch. 93A, § 2

Liability Triggers

State Law Claims

Massachusetts courts have laid out a number of helpful guideposts for determining when conduct is deceptive or unfair for purposes of Chapter 93A…conduct is "deceptive" when "**it has the capacity to mislead consumers, acting reasonably under the circumstances, to act differently than they otherwise would have acted**."…Both the defendant's and the plaintiff's conduct, knowledge, and what they should have reasonably known may be factors in determining whether an act or practice is unfair. Ultimately, "**Massachusetts leaves the determination of what constitutes an unfair trade practice to the finder of fact**, subject to the court's performance of a legal gate-keeping function."

Hanrahran v. Specialized Loan Servicing, LLC, 54 F. Supp. 3d 149, 154 (D. Mass. 2014)

Liability Triggers

State Law Claims: Illinois Biometric Information Privacy Act

Sec. 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

(Source: P.A. 95-994, eff. 10-3-08.)

Liability Triggers

Federal Trade Commission

- The FTC has brought actions against organizations that have violated consumers' privacy rights or misled consumers about data security. The FTC has charged organizations with violating Section 5(a) of the Federal Trade Commission Act for unfair or deceptive acts or practices affecting commerce.
- In addition to case law, statutes, and regulations, we can look to FTC Complaints and Consent Decrees for guidance on developing a standard of care to avoid claims.
- For example:
  - In the Matter of Snapchat
  - In the Matter of LifeLock, Inc.

Liability Triggers

Federal Trade Commission

- In the Matter of Snapchat – Deceptive Trade Practices
  - Snapchat marketed to consumers that short messages, or snaps, would only be stored for a short period of time before disappearing forever. In reality, the company had methods that could save chats indefinitely. There was also a Find Friends feature of Snapchat that was inadequately secured and resulted in the ability of hackers to obtain millions of Snapchat users' information.
  - As part of a settlement with the FTC, Snapchat was prohibited from misrepresenting the extent of how it maintains the privacy, security, or confidentially of users' information. The Company was also required to implement a comprehensive privacy program that would be monitored by an independent professional for the next 20 years.

- https://www.ftc.gov/system/files/documents/cases/140508snapchatcmpt.pdf
- https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

Liability Triggers

Federal Trade Commission

- In the Matter of LifeLock, Inc.– Unfair Trade Practices
  - In 2006, LifeLock advertised that it could protect consumers from all identify theft through its monthly services. FTC asserted that LifeLock could only protect against some forms of identify theft. LifeLock also failed to encrypt customer data putting the data at risk. In 2010, LifeLock settled with the FTC agreeing to pay $12 million. LifeLock also agreed to implement a comprehensive information security program to protect the customers personal data that would be assessed every two years.
  - In 2015, the FTC filed a contempt action against LifeLock asserting that LifeLock had failed to comply with the 2010 consent order as it had failed to maintain a comprehensive information security program to protect customers' personal information and continued to engage in deceptive advertising.
- https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states
- https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated

Liability Triggers

Contract

The Plaintiffs have failed to allege facts establishing the necessary elements of an implied contract claim. The Georgia Court of Appeals has explained that, for both express and implied contract claims, “[t]he concept of a contract requires that the minds of the parties shall meet and accord at the same time, upon the same subject matter, and in the same sense.” “In the absence of this meeting of the minds, there is no special contractual provisions between the alleged contracting parties.” An implied contract only differs from an express contract in the type of proof used to prove its existence. The same element of mutual assent is required. The Contract Plaintiffs allege that an implied contract was formed because “Equifax agreed to safeguard and protect the Personal Information of Plaintiffs and Class members and to timely and accurately notify them if their Personal Information was breached or compromised.” This conclusory allegation fails to establish the necessary element of mutual assent. This allegation, which contains a legal conclusion instead of a factual allegation, fails to show that the Defendants and the Contract Plaintiffs had a meeting of the minds, as required by Georgia law. Therefore, the Contract Plaintiffs' implied contract claim fails to state a claim.

In re Equifax, Inc., Customer Data Sec. Breach Litig.,

GOLDBERG SEGALLA

Risks

1. Bad People
2. Bad Education
3. Bad Technology

GOLDBERG SEGALLA

Pirata est hostis humani generis

- M. Tullius Cicero, De Officiis III, 107 44 B.C.

Simon Ledingham (CC BY-SA 2.0)

Cyber Pirates

- Organized Crime
- Nation States
- Terrorist Organizations
- Industrial Spies
- Hackers
- Hacktivists
- Insiders

GOLDBERG SEGALLA

Cyber-Arsenal

- Social Engineering
- Phishing / Spear Phishing
- Remote Access (Hardware)
- Remote Access (Software)
- Software Exploits
- Malware
- Ransomware
- Passwords Exploitation
- Brute Force Attacks

GOLDBERG SEGALLA

Bad Education

Digital Natives, Digital Immigrants

Marc Prensky

From *On the Horizon* (MCB University Press, Vol. 9 No. 5, October 2001)

It is now clear that as a result of this ubiquitous environment and the sheer volume of their interaction with it, today's students think and process information fundamentally differently from their predecessors. These differences go far further and deeper than most educators suspect or realize. "Different kinds of experiences lead to different brain structures," says Dr. Bruce D. Perry of Baylor College of Medicine.

GOLDBERG SEGALLA

Social Engineering

- According to Verizon's 2019 Data Breach Investigations Report (DBIR), social attacks resulted in approximately 33% of data breaches.
  - https://enterprise.verizon.com/resources/reports/dbir/

Social Engineering

- Phishing
  - The 2019 Verizon DMIR found that phishing attacks resulted in the plurality of breaches.
    - https://enterprise.verizon.com/resources/reports/dbir/2019/results-and-analysis/
- Whaling
  - The 2019 Verizon DBIR also found that C-level executives were twelve times more likely to be the target of social breaches than in the past.
    - https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

GOLDBERG SEGALLA

Social Engineering

- The risk for social engineering attacks is not limited to any specific sector. Those in a wide-range of industries face risks from social engineering including the public, professional, healthcare, and financial sectors. Individuals are also the targets of these attacks as well.

KnowBe4's Phish-Alert tool picks up spoofed campus-wide phishing attempt in Florida targeting a community college with a fake active shooter alert.

This particular phish spoofs a campus-wide security alert for a community college (confidential information blocked out) in Florida. If there is any saving grace with this phish, it lies with the awkward choice of language ("an emergency scare"), which should tip off most users that something is not right with this email. Those for whom English is second language might not pick up on that, though, and students whose native language is not English are quite common on college campuses.

According to KnowBe4 CEO Stu Sjouwerman, "Given that it appears to be tailored to a particular educational institution and its students and employees, it's a good bet that other educational institutions could see similarly targeted phishing attacks.

https://www.knowbe4.com/press/knowbe4-alerts-colleges-nationwide-against-active-shooter-alert-phishing-scam

Social Engineering

- If the failure to exercise ordinary care substantially contributes to a loss from a social engineering scheme, the individual who failed to exercise such care will likely be liable.
  - *See Bile v. RREMC, LLC*, 2016 WL 4487864 (E.D. Va, Aug. 26, 2016).
- However, this is an extremely fact-specific analysis and there is not a one-size fits all answer.

Social Engineering

- Similar issues can be found when dealing with fraudulent transfers. The U.C.C. provides additional guidance on this issue.
  - Under U.C.C. § 3-404:
    - (a) **If an impostor ... induces the issuer of an instrument to issue the instrument** to the impostor ... by impersonating the payee of the instrument or a person authorized to act for the payee, **an indorsement of the instrument by any person in the name of the payee is effective as the indorsement of the payee in favor of a person who, in good faith, pays the instrument** or takes it for value or for collection ....

Social Engineering

- Under U.C.C. § 3-404(d):
  - With respect to an instrument to which subsection (a) ... applies, **if a person paying the instrument or taking it for value or for collection fails to exercise ordinary care in paying or taking the instrument and that failure substantially contributes to loss** resulting from payment of the instrument, **the person bearing the loss may recover from the person failing to exercise ordinary care to the extent the failure to exercise ordinary care contributed to the loss.**
- When developing a standard of care to reduce or mitigate potential risk for social engineering schemes, one should be confident that they have, at a minimum, exercised **ordinary care**.

GOLDBERG SEGALLA

Bad Technology

Information Technology ≠ Information Security

GOLDBERG SEGALLA

Bad Technology

- No Anti-Virus
- Antique Anti-Virus
- Open Doors / Remote Access
- Outdated Software
- Useless Firewalls
- Log Deletion
- No-Factor Authorization
- One-Factor Authorization
- Stored Passwords
- Unregulated Passwords
- Unlimited Storage
- No Document Management
- Poor Device Management
- Personal Accounts
- On-Site Backups
- Cobbled Systems
- No Email Filters
- No Website Filters
- No Black Markers
- IT Amateurs
- Third-Party Amateurs

Reasonableness Guideposts

1. Statutory Requirements
2. Industry Requirements
3. Experts

- Generally, the United States views privacy issues from a sectorial model.
  - Unlike the GDPR, there is no overarching privacy law in the United States. Instead, there are many different rules, regulations, and statutes.
  - For example, each state might have its own rules related to what constitutes a breach incident and what is required for breach response.
  - Additionally each industry (e.g., financial, healthcare, or marketing) have their own standards.
- This is important to understand as when determining what one's digital duties might be necessary to develop an appropriate standard of care you could be dealing with dozens of different rules depending on the sector you are in, the data you hold, and the individuals involved.

Legal Profession

- Law offices are not immune to digital risks and duties.
- In 2012, the ABA amended Rule 1.6(c) of the Model Rules of Professional Conduct to incorporate cybersecurity concerns.
- "A lawyer shall make **reasonable efforts** to prevent the inadvertent or unauthorized disclosure, or unauthorized access to, information relation to the representation of a client."
- What factors constitute reasonable efforts?
- Comment 18 lists a variety of factors to consider to assess the reasonableness of an attorney's actions such as "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."

Legal Profession

- Some states have adopted the model rules or a variation of the rules. However, not surprising, the definition of reasonable varies.

1. **New York:**
    - Four steps to consider in determining reasonable care: (1) “[e]nsuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security”, (2) investigating the provider's own security measures, (3) using available technology to prevent foreseeable infiltration attempts, and (4) looking into the provider's ability to erase data after the business relationship is terminated.
    - https://nysba.org/ethics-opinion-1019/

Legal Profession

2. **Massachusetts:**
    - As it relates to using a service such as Google Docs, reasonable efforts include examining the provider's policies and procedures, making sure the terms of use prohibit unauthorized access, ensuring that the lawyer has access to the data past termination of the use of service, examining the provider's own cybersecurity efforts, and staying up to date with all of the above.
    - https://www.massbar.org/publications/ethics-opinions/ethics-opinions-2012-opinion-12-03
3. **Iowa:**
    - The Iowa opinion sets forth questions that lawyers should ask when considering using information technology services, including accessibility inquiries on access, legal issues, financial obligations, and termination of services, and data protection inquiries on password protection, public access, and data encryption.
    - Ethics Opinion 11-01

Healthcare Industry

- **HIPPA Privacy Rule**
  - “The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.”
  - https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

- **HIPPA Security Rule**
  - The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. ”
  - https://www.hhs.gov/hipaa/for-

Healthcare Industry

- Although HIPPA does not provide an individual with a private right of action, an individual may still have a claim under a state negligence theory. When that is the case, courts have looked to the regulations implemented by DHHS for context as to the question of an applicable standard of care. Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C., 314 Conn. 433, 102 A.3d 32 (2014).

Healthcare Industry

1. Administrative Safeguards: 45 CFR § 164.308
    - Security Management Process
        - Have policies and procedures in plan to prevent security violations.
    - Security Personnel
        - Designate a person responsible for the development and implementation of the security management process.
    - Information Access Management
        - Have policies in place regarding authorization of access to ePHI.
    - Workforce Training and Management
    - Evaluation
        - Periodic evaluations to determine if policies are meeting the relevant standards.

Healthcare Industry

2. Physical Safeguards: 45 CFR § 164.310
    - Facility Access and Control
        - Limited access of facilities, both physical and electronic, to ensure information is only accessed by authorized individuals.
    - Workstation and Device Security
        - Implement policies to ensure workplaces are secure and information is only accessed by authorized individuals.

Healthcare Industry

3. Technical Safeguards: 45 CFR § 164.312
    - Access Control
        - For example, have appropriate software in place.
    - Audit Controls
        - For example, have appropriate software in place that can record and examine the use or access of ePHI.
    - Integrity Controls
        - Have procedures to protect ePHI from unauthorized alteration or destruction.
    - Transmission Security
        - Have technology in place to avoid unauthorized access of electronic transmission of ePHI.

Financial Industry

- GLBA and FTC
- Privacy and Safeguards Rule
- FACTA Disposal Rule
- NY DFS Cybersecurity Regulation

Privacy Rule

- Gramm-Leach-Bliley Act.
- Requires financial institutions to give customers clear and conspicuous written notice describing their privacy policies and practices.
  - 16 CFR § 313.
- The notice must be provided initially (when the customer relationship is established) as well as annually as long as the relationship exists.
- Specifically, the notice should contain information about how nonpublic personal information is collected, disclosed, and protected.

- Applies to Financial Institutions
  - 16 C.F.R. 313.3(k)(1)
    - Financial institution means any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution
  - 16 C.F.R. 313.3(k)(2) Examples of financial institution
    - (viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act

Safeguards Rule

- In addition to the Privacy Rule, the GLBA also contains a Safeguards Rule. The rule applies to the handling of customer information by all financial institutions which the FTC has jurisdiction.
  - 16 CFR § 314.
- The Safeguards Rule requires financial institutions to have measures in place to keep customer information secure. This not only requires financial institutes to safeguard customer information, but also requires financial institutions to ensure that its affiliates and service providers are safeguarding customer information placed in their care.

Safeguards Rule – Security Plan

- Develop a written information security plan and program to protect customer information
  - Must be appropriate to the company's size and complexity,
  - the nature and scope of its activities, and
  - the sensitivity of the customer information it handles

Safeguards Rule

- The Safeguards Rule contains a number of elements financial institutions must to develop, implement, and maintain its information security program. Those include:
  - (a) Designate an employee or employees to coordinate your information security program.
  - (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

    (1) Employee training and management;

    (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

    (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

Safeguards Rule

- (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- (d) Oversee service providers, by:

  (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

  (2) Requiring your service providers by contract to implement and maintain such safeguards.
- (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
- 16 CFR § 314.4.

Safeguards Rule – Safeguards

- Employee Training and Management
  - Background Checks and NDAs
  - Control and Limit Access (Remote and Local)
  - Robust Device and Strong Password Policy
  - Training…Training…Training…and Discipline
- Information Systems
  - Inventories, Encryption and 3-2-1 Backups
  - Air-Gapped and Secure Rooms, Networks, Servers and Systems
  - Use/Update Security and Intrusion Software and Hardware
  - FTC Disposal Rule (16 C.F.R. Part 682)
- Managing System Failures

See IRS Publication 4557: Safeguarding Taxpayer Data

Safeguards Rule – Flexibility

The requirements are designed to be **flexible**. Companies should implement safeguards **appropriate to their own circumstances**. For example, some companies may choose to put their safeguards program in a single document, while others may put their plans in several different documents — say, one to cover an information technology division and another to describe the training program for employees. Similarly, a company may decide to designate a single employee to coordinate safeguards or may assign this responsibility to several employees who will work together. In addition, **companies must consider and address any unique risks raised by their business operations — such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network**

https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying#how

FACTA Disposal Rule

- "Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." 16 CFR § 682.3 (a).
- What are "reasonable" measures?
  - For example: implementing and monitoring compliance with policies related to destruction of papers, erasure of electronic medical, and contracting with third parties regarding destruction of materials. 16 CFR § 682.3 (b).

NY DFS Cybersecurity Regulation Covering the Financial Services Sector

- 23 NYCRR 500 – went into effect in March 2017 and is now fully in force
- CPA firms are not directly affected (as they are not regulated by the NY DFS), but many of their clients and employers will be, such as:
  - Licensed lenders
  - State-chartered banks
  - Trust companies
  - Service contract providers
  - Private bankers
  - Mortgage companies
  - Insurance companies doing business in New York
  - Non-U.S. banks licensed to operate in New York

NY DFS Cybersecurity Regulation

- To effectively counsel these businesses, CPA firms should understand this regulation! CPAs need to be aware of what their clients and employers need to do to comply with the new regulations and make sure they leave themselves enough time to do so

GOLDBERG SEGALLA

NY DFS Cybersecurity Regulation

- All entities regulated by DFS must:
  - Perform initial risk assessment and then establish a cybersecurity program and implement cybersecurity policies
  - Provide notice to the DFS of a cybersecurity event
  - Establish policies for disposal of nonpublic info that is no longer needed
  - Limit and periodically review access privileges
  - Conduct periodic risk assessments
  - Implement policies and procedures to ensure 3rd party service provides are securing info accessible to them

NY DFS Cybersecurity Regulation

- And, unless the limited exemption applies (not a total exemption), entities must also:
  - Designate a Chief Information Security Officer
  - Train employees and monitor authorized users
  - Develop an incident response plan
  - Establish multi-factor authentication
  - Conduct penetration testing and vulnerability assessments
  - Establish procedures and guidelines for in-house developed applications
  - Encrypt data at rest and in transit
  - Establish an audit trail
- Limited exemption applies to covered entities with fewer than 10 employees (including independent contractors and affiliates) that are based or direct business in New York, less than $5 million in gross revenue from New York business operations, or less than $10 million in year-end total assets. Must give notice to DFS within 30 days of determination that limited exemption applies to the entity

GOLDBERG SEGALLA

GDPR Security Principles

- Privacy by design
  - Default mode of operation for businesses
  - Must be designed as such at the beginning
- GDPR's seven principles:
  - Obtain data lawfully, fairly and be transparent
  - Be honest about why you are collecting data
  - Minimize the data you need to collect
  - Update the data you collect with the most recent information
  - Delete after intended use
  - Maintain data integrity and security
  - Record your compliance efforts

State Law Considerations

Ohio Safe Harbor Provision

Ohio passed a bill which provides a “safe harbor”, which is an “affirmative defense”, to tort claims arising out data breaches caused by third-party malefactors. The bill indicates that all covered entities (any Ohio business that “…accesses, maintains, communicates, or handles personal information”), may seek a safe harbor under the law provided the company has a “written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information that complies with the NIST cybersecurity framework or other industry cybersecurity frameworks.

https://www.ohiosenate.gov/senators/hackett/news/hackett-bill-aimed-at-incentivizing-increased-cybersecurity-for-businesses-signed-by-governor

State Law Considerations

Encryption Protection

- Alabama – S.B. 318 / Act 2018-396 (the “Data Breach Notification Act”)
  - Excluded from Personally Identifiable Information
- Alaska – Alaska Stat. §45.48.010 *et seq.* (Personal Information Protection Act)
  - “personal information” means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired,
- Arizona – Ariz. Rev. Stat. § 18-551 et seq.
  - "Breach" or "security system breach": (a) Means an unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of unencrypted and unredacted computerized personal information
- Arkansas – Ark. Code § 4-110-101 *et seq.* (Personal Information Protection Act)
  - Threshold to Notify – 4-110-105 (a)(1) Any person or business that acquires, owns, or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to any resident of Arkansas whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

State Law Considerations

Encryption Protection

- California - Cal. Civ. Code § 1798.29 (state agencies), § 1798.82 (business entities)
  - Threshold to Notify & Timing – 1798.82(a)
    (a) A person or business …shall disclose a breach of the security
    (1) whose unencrypted personal information…or,
    (2) whose encrypted personal information …and the encryption key
- Florida – Fla. Stat. § 501.171, (see also § 282.003 et seq. ("Information Technology Management Act")
  - § 501.171(1)(g)(2) "personal information"…The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

ALL 50 STATES HAVE THIS CARVE OUT…
…SO WHY NOT ENCRYPT YOUR DATA?

State Statutes –

Illinois Biometric Data

§ 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

P.A. 95-994, § 15, eff. Oct. 3, 2008 / 740 Ill. Comp. Stat. Ann. 14/15

Illinois Biometric Data

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.
(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:
(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;
(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;
(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or
(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.
(e) A private entity in possession of a biometric identifier or biometric information shall:
(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and
(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.
Credits

P.A. 95-994, § 15, eff. Oct. 3, 2008. / 740 Ill. Comp. Stat. Ann. 14/15

GOLDBERG SEGALLA

Payment Card Industry Data Security Standard (PCI DSS)

1. Build and Maintain a Secure Network and Systems
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

GOLDBERG SEGALLA

National Institute of Standards and Technology

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0 (April 2018)

Following three slides taken directly from:
https://www.nist.gov/cyberframework/framework

The Cybersecurity Framework

Three Primary Components

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

Implementation Tiers

A qualitative measure of organizational cybersecurity risk management practices

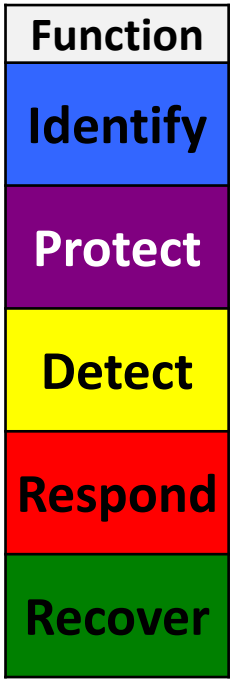
Key Framework Attributes

Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector

The Framework Core

Establishes a Common Language



- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Center of Internet Security Critical Security Controls

1. Inventory of Authorized and Unauthorized Software
2. Inventory of Authorized and Unauthorized Devices
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, monitoring, and Analysis of Audi Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols and Services
10. Data Recovery Capability

Center of Internet Security Critical Security Controls

11. Secure Configurations for Network Devices such as Firewalls, Routers and Switches
12. Boundary Defense (Detect, prevent and correct the follow of information)
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Read Team Exercises

https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf

Ask the Experts

Overall, according to cybersecurity experts, a “catastrophic breach of Equifax's systems was inevitable because of systemic organizational disregard for cybersecurity and cyber-hygiene best practices.”

In re Equifax Inc. Sec. Litig., 357 F. Supp. 3d 1189, 1207 (N.D. Ga. 2019)

Emerging digital security standards are particularized and case specific. Unlike prior specific requirements, such as passwords or firewalls, the new corporate security obligation is fact-specific, requiring companies to go through a “process” and determine what security measures are most appropriate for the company's security needs. Allows companies to create their own specific security measures so long as the companies conduct ongoing reviews of their security mechanisms.

See e.g. Thomas J. Smedinghoff, An Overview of Data Security Legal Requirements for All Business Sectors 4-6 (Oct. 8, 2015) (collecting cases) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2671323

GOLDBERG SEGALLA

May 1, 2018

Building a world without passwords

Microsoft Security Team

When we think about creating a world without passwords, we want to deliver on two key promises:

1. **User promise**: *End-users should never have to deal with passwords in their day-to-day lives.*

2. **Security promise**: *User credentials cannot be cracked, breached, or phished.*

At its core, our fundamental philosophy is simple: **devalue the password**, and replace it with something that eradicates its use for the end user and drains its value for an attacker.

https://www.microsoft.com/security/blog/2018/05/01/building-a-world-without-passwords/

More than 99.9 percent of Microsoft enterprise accounts that get invaded by attackers didn't use multi-factor authentication (MFA). This stark, though not entirely surprising, finding comes from a presentation that Alex Weinert, the tech giant's Director of Identity Security, delivered at the RSA 2020 security conference in San Francisco in late February. Overall, **only 11 percent of Microsoft enterprise accounts had MFA enabled**.

March 9, 2020

https://www.welivesecurity.com/2020/03/09/microsoft-99-percent-hacked-accounts-lacked-mfa/

Google 2-Step Verification (website)

It's easier than you think for someone to steal your password

Any of these common actions could put you at risk of having your password stolen:

- Using the same password on more than one site
- Downloading software from the Internet
- Clicking on links in email messages

2-Step Verification can help keep bad guys [sic] out, even if they have your password.

https://www.google.com/landing/2step/#tab=why-you-need-it

Professor L. Jean Camp

Evaluating User Perception of Multi-Factor Authentication: A Systematic Review

To mitigate single point failures, new and technologically advanced Multi-Factor Authentication (MFA) tools have been developed as security solutions. However, the usability and adoption of such tools have raised concerns…Our meta-analysis of user focused studies (n = 57) showed that researchers found **lower adoption rate to be inevitable for MFAs, while avoidance was pervasive among mandatory use**.

https://arxiv.org/ftp/arxiv/papers/1908/1908.05901.pdf

GOLDBERG SEGALLA

Professor L. Jean Camp

MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content

Multi-factor authentication (MFA), intends to enhance security by providing additional verification steps. **However, in practical deployment, users often experience dissatisfaction while using MFA, which leads to non-adoption**…While some users acknowledge the security benefits of MFA, majority of them still faced problems with initial configuration, system design understanding, limited device compatibility, and risk trade-offs leading to non-adoption of MFA. Based on these results, we provide actionable recommendations in technological design, **initial training, and risk communication** to improve the adoption and user experience of MFA

https://arxiv.org/ftp/arxiv/papers/1908/1908.05902.pdf

GOLDBERG SEGALLA

Encryption…

GOLDBERG SEGALLA

Examples & Explanations

GOLDBERG SEGALLA

Best Practices

GOLDBERG SEGALLA

People & Processes

- CISO / IT Management / Dedicated Security
- Privacy Policy / Response Plan
  - Employment Lifecycle / Data Lifecycle
- Mandatory and Appropriate Training, Drills and Discipline
- Principle of Least Privilege
- Data Mapping / Data Hiding
- Document Management / Shredding Policy
- Back-Channeling and Paper Checks
- Password Management
- Cyber-Hygienic Culture / Real-Time Reporting
- Security Assessments and Audits
- Vendor Management and Contract Coordination

GOLDBERG SEGALLA

Networks and Systems

- Network Engineering and Firewalls
- Secure Email / File Sharing
- Patches and updates
- SPAM / malicious email filter
- Trusts and website filter
- Scan for malware
- Scan for intrusions / access
- Complex (Strong) Passwords
- Desktops vs. Workstations
- Device Settings (BYOD)
- Multi-factor authentication
- Close ports on computers
- Remote Desktop / access
- Disable Office 365 accounts
- Limit remote access to trusted devices via encrypted connections
- Penetration testing
- Data mapping and audits
- Air-Gaps
- 3-2-1 Backups
- Generate and Maintain Logs
- Data Preservation
- Vendor Coordination

Vendor Agreements

- Review Vendor / Supplier Contracts
  - Indemnity Language
  - Limitations on Damages / Warranties / Time
  - Vendor Insurance / Additional Insured Status
  - Defined Security Requirements, Compliance and Audits
  - Notice Provisions
  - Incident Response Management
  - Confidentiality
  - Choice of Law / Venue / Jurisdiction
  - Dispute Resolution

Questions?

- **James M. Paulino, II, Esq.**
- 585.295.8351| jpaulino@goldbergsegalla.com

- **Michael A. Goode, Esq., CIPP/US**
- 919.582.0819 | mgoode@goldbergsegalla.com