KROLL

A Reasonable Approach to Data Security

November 3, 2022

Table of Contents

Meet the Panelists

Sadia Mirza
Associate
Troutman Pepper

Justin Price
Associate Managing Director
Kroll

Alex Pearce
Partner
Wyrick Robbins

Sam Jacobs
Associate Managing Director
Kroll

Shea Leitch
Of Counsel
Squire Patton Boggs

What is a Reasonable Approach to Data Security?

- There is no single, comprehensive federal law regulating data security in the United States (same goes for privacy – but that's a conversation for another date).
- Rather, at the federal level, the U.S. has taken a sectoral approach to data security.
- At the state level, several states have enacted their own data security laws, and all states have enacted their own data breach notification laws.
- Embedded within almost all these laws is the concept of "reasonable" security.

It’s a Potpourri - State of Data Security Laws

Data security laws generally fall into one or more of the following categories:

- The “Reasonable Security” Approach
- The Prescriptive Approach
- The Carrot, Not the Stick, Approach

The “Reasonable Security” Approach

Sector Specific Data Security Rules and Laws

- Gramm-Leach-Bliley Act (GLBA) Safeguards Rule
- FTC Safeguards Rule
- HIPAA Security Rule
- Fair Credit Reporting Act

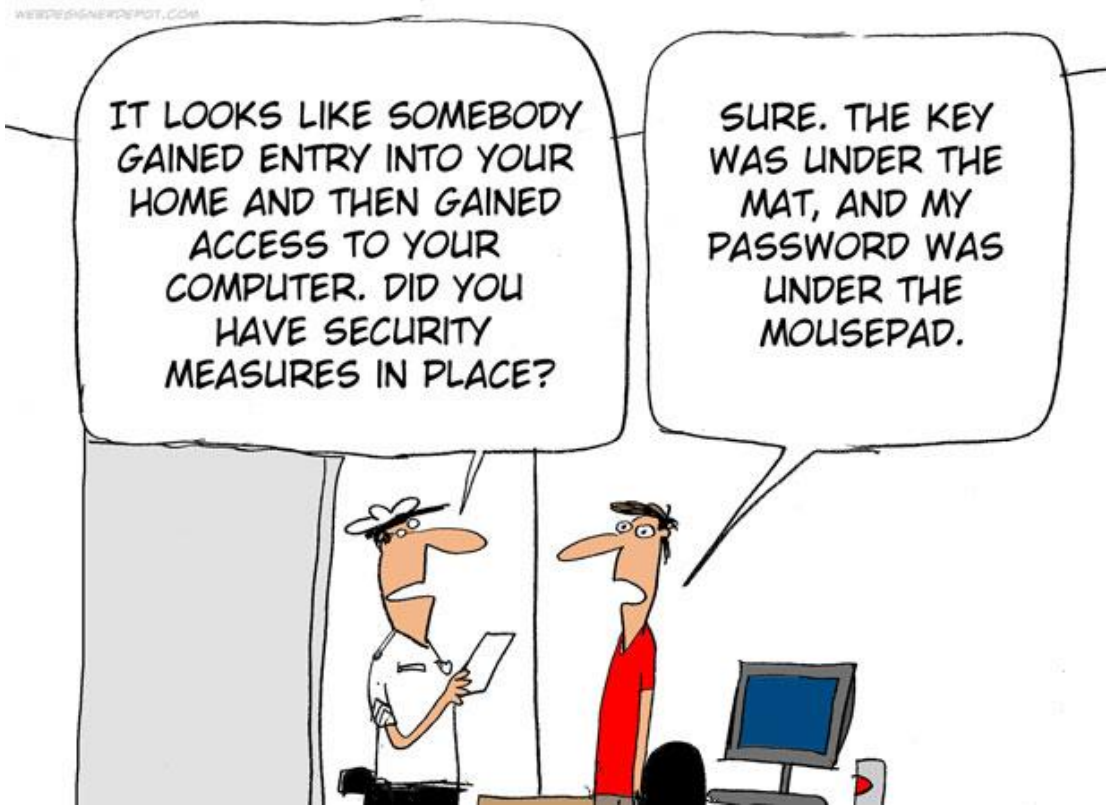
The “Reasonable Security” Approach

State Data Security Laws

- Approximately twenty-two (22) states follow the “reasonable security” approach to data security in that they require businesses to maintain reasonable security procedures and practices to protect certain “personal information” from unauthorized access, destruction, use, modification, or disclosure.
  - Examples:
    - California: Cal. Civ. Code § 1798.81.5
    - Florida: § 501.171(2), Fla. Stat.
    - Texas: Tex. Bus. & Com. Code Ann. § 521.052(a)

Is the “Reasonable Security” Approach Reasonable?

- Reasonableness in data security is required given how rapidly the cyber landscape and information technology are changing.
- Confirms that no single data security strategy or set of controls works effectively in all situations.
- Avoids static requirements that may become outdated as technologies and threats change.
- Provides organizations with options based on their size, complexity, resources, and the nature of their activities and the data they collect and use.



Determining What's Reasonable – No Fixed Standard

- Industry Guidelines and Frameworks
- Risk Assessments
- Informal Regulator Guidance (e.g., FTC "Start with Security" Guide; CA AG's 2016 Data Breach Report)
- Regulatory Enforcement Actions (e.g., FTC settlements)

The Prescriptive Approach

Does this Make Data Security Easier, Harder, Better?

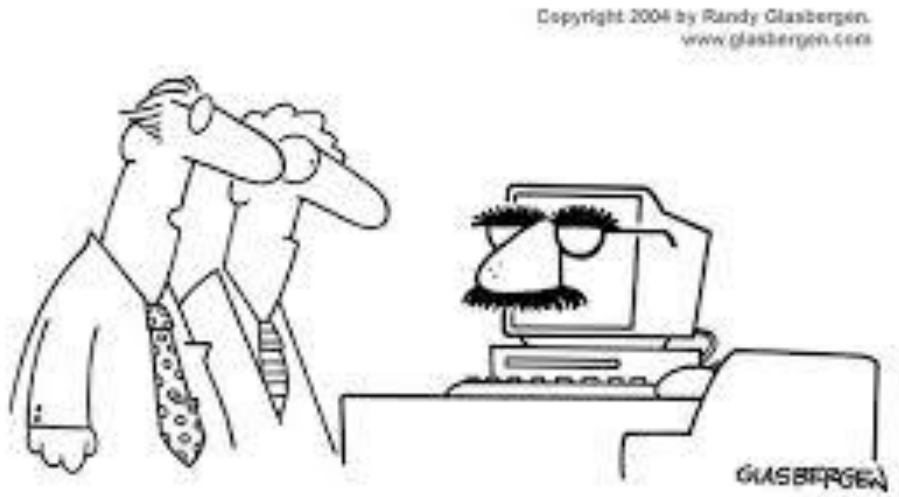
- Massachusetts Standards for the Protection of Personal Information
- Oregon and New York (SHIELD Act)
- Minnesota, Nevada, and Washington - PCI DSS
- Amended FTC GLBA Safeguards Rule
- NY DFS Cybersecurity Regulations

The Prescriptive Approach

Does this Make Data Security Easier, Harder, Better?

Dissenting Statement of Commissioner Noah Joshua Phillips and Commissioner Christine S. Wilson to the Proposed Modifications to the Safeguards Rule – March 5, 2019

- "The Rule as written provide direction to financial institutions on how to protect data security—importantly, while not being overly prescriptive—in an area where standards continue to evolve. The current proposal, however, trades flexibility for a more prescriptive approach, potentially handicapping smaller players or newer entrants."
- "[T]he Safeguards Rule today is a flexible approach, appropriate to a company's size and complexity. This proposal would move us away from that approach . . . The proposed precautions, either individually or in the aggregate, may constitute best practices for certain n firms. But the proliferation of procedural, technical, and governance requirements may have the unintended consequence of diluting core data security measures undertaken pursuant to the existing Safeguards Rule."



"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

The Carrot, Not the Stick Approach

- Under this approach, the law incentivizes the adoption of industry recognized cybersecurity frameworks by providing an affirmative defense or other similar “safe harbors” against claims arising in litigation from a data breach.
- Frameworks cited in these laws include NIST standards, ISO 2700 series, FedRAMP, and CIS Critical Security Controls.
- Examples include:
  - Ohio
  - Utah
  - Connecticut

A Practical Roadmap for Reasonable Security

Risk-Based Approach

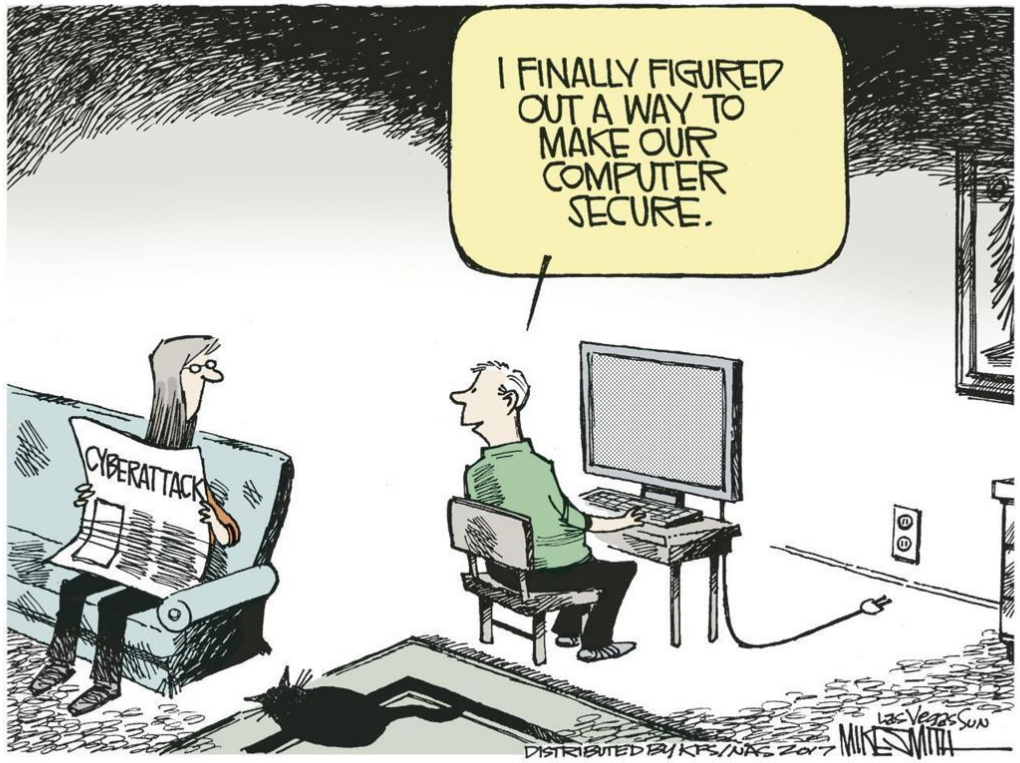
- There is no “one size fits all” solution to cybersecurity risks.
- Determining whether a company had reasonable cybersecurity measures cannot be based solely on whether the company prevents an incident.
- Whether a company used reasonable cybersecurity measures, one must look at all four aspects of their cybersecurity programs:
  - Prevention
  - Detection
  - Containment
  - Remediation
- Practical considerations:
  - Size of the company
  - Nature of data collected
  - Industry
  - Complexity

https://wyzguyscybersecurity.com/sunday-funnies-security-edition/

Reasonable Measures

Risk-Based Approach

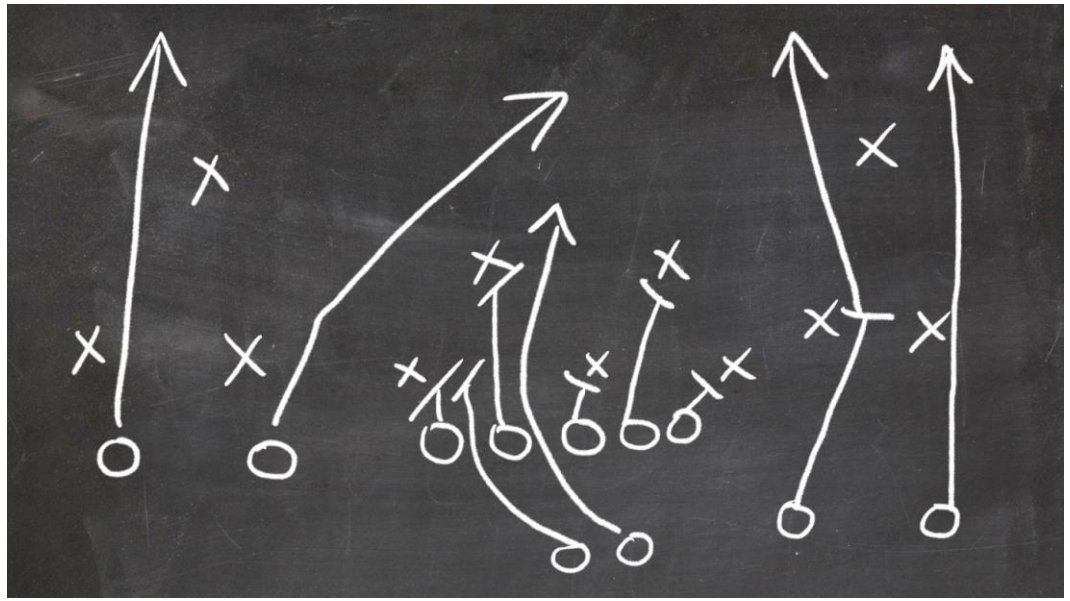
- The U.S. National Institute of Standards & Technology ("NIST"), in its Cybersecurity Framework, recommends a "risk-based approach" to cybersecurity
  - "Enables an organization to gauge the resources needed (*e.g.*, staffing, funding) to achieve cybersecurity goals in a cost-effective, prioritized manner."[1]
- Risk-based approach recognizes that there is no single checklist that a company must or should follow.
- Risk-based approach dictates that companies allocate resources to cybersecurity based on risk levels and *balance* security with business functionality.
- Reasonable security is about tradeoffs and return on security investment to provide "the most security, for the greatest number of users, the vast majority of the time."[2]



Reasonable Measures

Policies and Procedures

- Cybersecurity Policies and Procedures
  - Eight important “Are they” questions about P&Ps:
    - Based on a recommended framework?
    - Documented?
    - Aspirational?
    - Comprehensive?
    - Funded?
    - Updated?
    - Understood?
    - Followed?
  - Polices and procedures are important but not the “end all be all” of an organization's cybersecurity maturity.
    - Important to evaluate what was actually being done by the employees.



Reasonable Measures

Best Practices

- While any security program must be tailored to a company's unique risk profile, best practices generally address the following elements:
  - Business Continuity Planning
  - Asset And Vendor Management
  - Threat Intelligence
  - Penetration Testing
  - Logging And Monitoring
  - Encryption
  - Data Sanitization
  - Secure Product Development
  - Vulnerability Management
  - Physical Security
  - Incident Response Management

https://ifunny.co/picture/when-your-security-posture-strategy-is-only-for-compliance-1EmKlMun8

Frontline of Defense – Employees

Data Security – Parting Thoughts

- Data security is an ongoing process.
- A company's data security procedures must be reasonable and appropriate in light of the circumstances.
- A breach does not necessarily show that a company failed to have reasonable security measures.
  - There is no such thing as perfect data security.
- A company's practices may be unreasonable even if no breach occurs.

Questions

KROLL