CONSTANGY
BROOKS, SMITH & PROPHETE LLP

Best Practices in Crisis Response to a Data Security Breach

Lindsay B. Nickle

Constangy Cyber Team

May 1, 2024

Evolving Risk

"[D]ata is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry.

If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world."

Ginni Romety
Chairman, President, CEO
IBM (2015)

Threat Landscape

The Most Pressing Risks

Most Common Threats

- **Ransomware**
  - Malicious software used by threat actor groups to attempt to extort a monetary payment
  - The greatest threat across all sectors
  - Business interruption and potential data breach
- **Business Email Compromise (BEC)**
  - Compromise of email accounts
  - Common goal of Committing financial fraud
  - Sophisticated phishing attacks and credential harvesting
  - Intercepting financial transactions
  - Social engineering
  - Potential Data Breach
- **Other Threats**

What is a Data Breach?

Definition: Data Breach

The unauthorized access or acquisition of legally protected data that compromises the security, confidentiality, or integrity of sensitive or legally protected personal information.

Definition: Personal Information

Generally, Personal Information (PI) is an individual's First Name or First Initial and Last Name, in combination with:

- **Social Security number**
- **Driver's License number**
- **Financial account number with means to access**
- **Health insurance or medical treatment information**
- **Email address/username in combination with password or security question**
- **Other information (varies by state)**

The Impact of the Regulatory Environment

- **State Regulations**
  - Variations among the state data breach notification statutes – All cover electronic, 10 also cover paper
    - Notification of consumers
    - Required timing and content of notification
    - Required regulatory notification
- **State Data Privacy Legislation**
  - CCPA and many similar enactments
- **State Information security standards**

The Impact of the Regulatory Environment

- **Federal Regulations and "Guidance"**
  - GLBA; SEC; HIPAA; FinCEN, OFAC, etc.
- **Industry Regulations**
  - PCI DSS
- **Contractual Relationships**
  - Requirements to notify regarding security incidents and data breaches
  - Contract management

Financial Implications

- **First-party costs**
  - Data loss; software loss; hardware loss
  - Income loss; business interruption costs; restoration costs
  - Cyber extortion; other crime loss.
- **Third-party costs**
  - Media liability (copyright and trademark infringement); privacy liability; bodily injury
  - Defensive litigation: class actions; derivative actions; and regulatory actions.
- **Remediation costs**
  - Legal services; forensics services; crisis management services; notification costs; credit monitoring and identity theft protection services.
- **Fines and penalties**
  - Expenses of regulatory investigations; civil judgments; fines and penalties levied by regulatory authorities.

Anatomy of a Data Breach

The Anatomy of a Data Breach

- **Discovery of Incident**
- **Forensics Investigation**
- **Detection of Data Impact**
  - Potential data impact in the event of a business email compromise
  - Potential data impact in a ransomware situation
- **Analysis of Data Impact**
- **Assessment of potential consumer and regulatory notification obligations**
- **Assessment of contractual and business partner notification obligations**

The Anatomy of a Data Breach

- **Complete the legal notification of individuals**
  - Engage notification vendor
  - Draft legally compliant consumer notification letters
  - Facilitate response to escalated consumer inquiries
  - Draft legally compliant regulatory notification letters
  - Interface with regulatory officials
- **Communication with vendors or business partners**
  - Analysis of contracts to determine notification obligations
  - Business impact as a communication driver
  - Press releases or media contacts

Communication Concerns

- **Choose your words carefully**
  - Avoid words that raise concerns, like breach, hacker, or ransomware
- **Consider whether public communication is necessary**
  - Operational impact
  - The gossip factor
  - Prepare internal and external communications plan
- **Selective transparency**
  - Be truthful, but selective in communication
  - Business impact as a communication driver
  - Press releases or media contacts

Questions?

How to Reach the Constangy Cyber Team:

24/7 Hotline and Response

877.DTA.BRCH (877-382-2724) |
BreachResponse@constangy.com

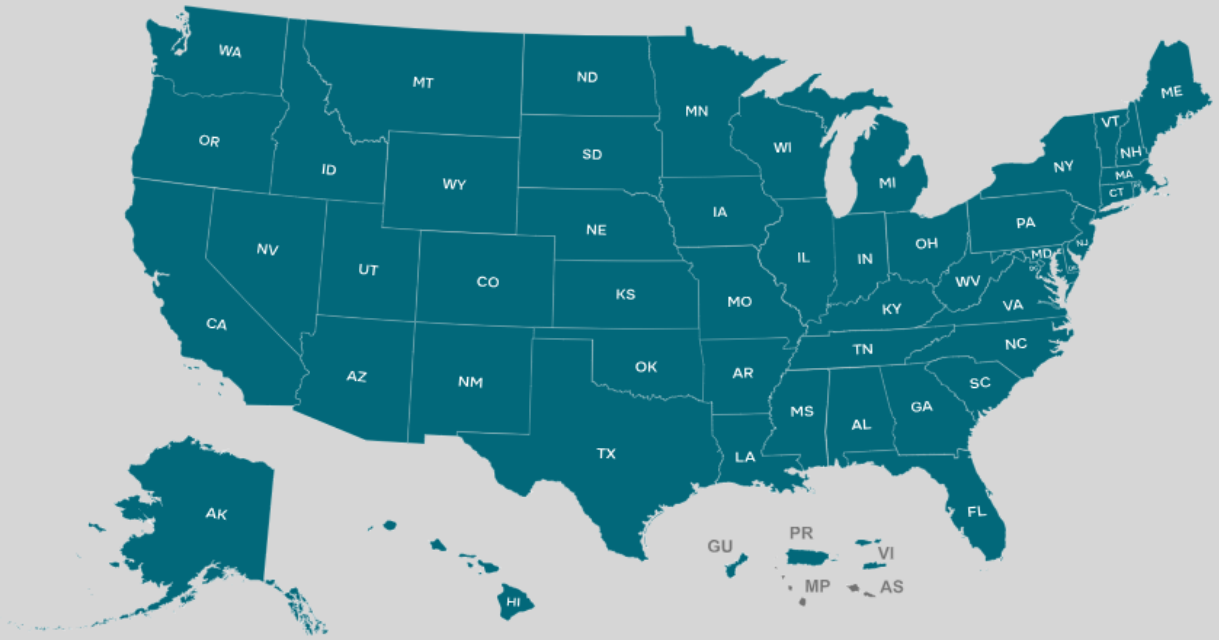
Lindsay Nickle | lnickle@constangy.com | 806-535-0274 (m)

Data Privacy Map - United States

BACK TO WORLD MAP

The **Constangy Cyber Team** understands the paramount importance of staying informed about the intricacies of data breach notification regulations. With our Cybersecurity & Data Privacy Desktop Reference and these interactive maps, we provide guidance to navigate these complexities. Our interactive maps offer you online access to our succinct summaries of the essential aspects of various consumer and regulatory notification obligations. Please contact us should you have any questions. We look forward to working with you should you have to navigate the consumer notification and/or regulatory reporting process.

- Search By Region / State -



For more information, and to subscribe to our cyber and data privacy blog, please scan the code :

CONSTANGY
BROOKS, SMITH &
PROPHETE LLP

Thank you!

https://www.constangy.com/practices-Cybersecurity-Data-Privacy