Cyber Law

July 21, 2022

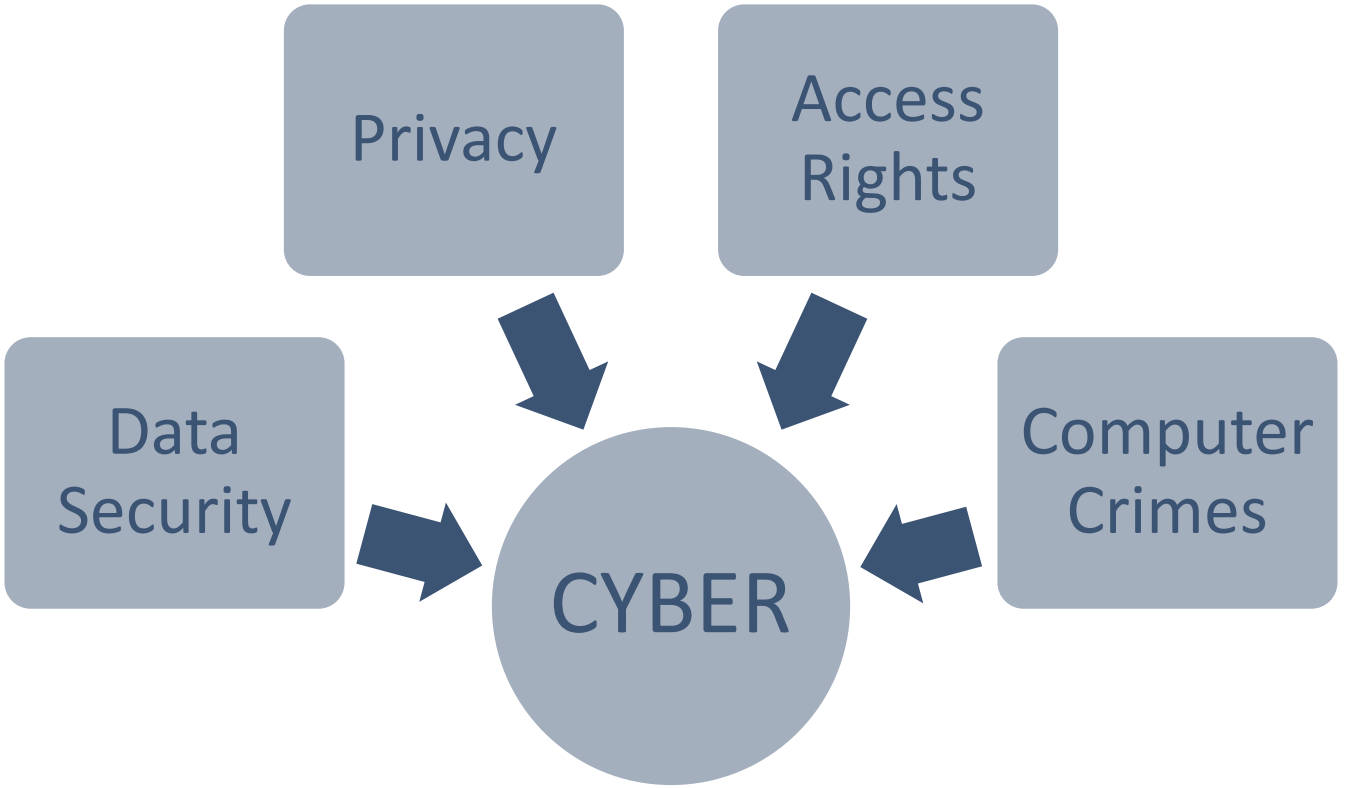
Sarah W. Anderson

AGENDA

- What is Cyber Law?
- Key Concept: Difference between Privacy and Data Security
- What are Cyber Incidents?
- Reliable Categorical Rules For Cyber Incidents
- The Lawyer's Role
- Regulated Data
- What is ESF-17?
- Questions & Answer

WHAT IS CYBER LAW?

Cyber Law is a collection of several regulations and individual rights:



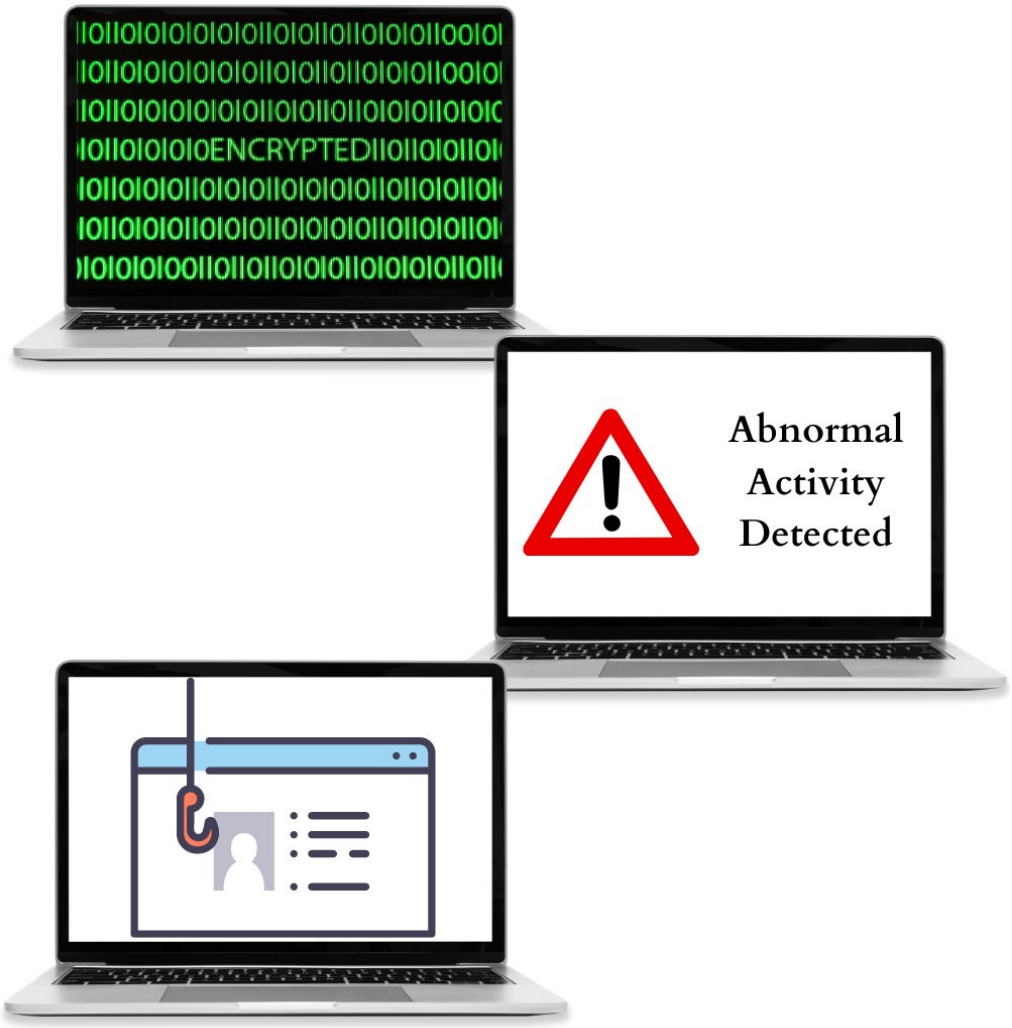
KEY CONCEPT

Security v. Privacy

Security	Privacy
The availability and integrity of data.	The appropriate use and control and data.
The protection against unauthorized access.	The protection against personally identifiable information.
Applies to all types of data and information that is stored electronically.	Specific to individuals and organizations – information that can identify them.
Security can be achieved without privacy.	Privacy requires security.
3 components: physical security of premises, administrative security, and digital security.	Focuses on how data is processed, how long it is held, where it is held, and who can hold it.

CYBER INCIDENTS

- There is no globally-accepted definition of a "cyber incident."
- Some definitions will focus on "breaches" versus cyber-attacks and ransomware events.
- Generally, cyber incidents include some, or all, of the following types of activity:
  - Indicators of compromise (in any form)
  - Complete encryption
  - Ransomware
  - Data breaches / Data Theft
  - Service interruptions
- Different types of cyber incidents may invoke different types of legal requirements.



CATEGORICAL RULES

1. **Call law enforcement.**
   WHY? Forensic assistance from law enforcement is FREE and information shared with them does not waive any legal rights or privileges under both federal and state Cybersecurity Information Sharing Act laws.
2. **Record every aspect of the event.**
   WHY? Details are important to law enforcement looking for trends, predicting behavior of any bad actors, and determining specific details of the incident.
3. **Do not provide any unnecessary public comments.**
   WHY? Cyber criminals read the news and look for what victims are saying about the incident. Also, do not want to waive any public records exceptions or compromise law enforcement investigations.
4. **Leave the computers on unless told otherwise by technology professionals.**
   WHY? Preserves evidence of the activity that is occurring.
5. **Be involved and ask questions of the technology experts.**
   WHY? Thorough legal advice and analysis cannot be given in a vacuum. Attorneys need to watch for potential spoliation claims, breach notification concerns, impacts on regulated data, and activities that may affect any insurance claim.

LAWYER'S ROLE

- Continues to evolve as case law sets new precedent every few months.
- Examine the matter from a fiduciary duty and due diligence perspective:
  - *Are the actions being taken contributing to a potential negligence claim?*
  - *Look for ways to mitigate liability:*
    - Involve law enforcement quickly
    - Conduct a thorough forensic examination of the issue
    - Rebuild better to prevent future events
- Look for the following issues:
  - Is what is happening going to jeopardize my client's ability to maintain privilege or confidentiality?
  - Is there any regulated data potentially exposed or stolen?
  - What information is being communicated to third parties?
  - Who are the vendors involved in this matter and what do the contracts with those vendors say?

REGULATED DATA

Educational Data:

- Family Educational Rights and Privacy Act (FERPA) – 1974 protects the privacy of student educational records. Applies to all schools that receive $ from the U.S. Department of Education. Prohibits disclosure of personally identifiable information absent written consent that specifies the records, the purpose of disclosure, and approved recipient subject to certain exceptions (i.e.: financial aid applications, transfer, accreditation).

Data Affecting Minors:

- Children's Online Privacy Protection Act (COPPA) requires websites, online services directed to kids under 13 to disclose the information it collects, how it's used, and how disclosed, and obtain verifiable parental consent. Also requires reasonable measures to protect the data. Penalties: $41K+ per violation.

Health Data:

- The Health Insurance Portability and Accountability Act (HIPAA) implements both Security and Privacy rules, with access rights conferred by the 21st Century Cures Act and Interoperability Rules.

Financial Data:

- Gramm Leach Bliley Act requires minimum "Safeguards" for any institution that performs financial services (recently expanded), such as having an information security plan that describes protections of customer information.

Biometric Data:

- Prohibits the collection of biometric info absent signed, written release with specific purpose for collection and duration information will be retained. Forbids the sale, lease, or profit of info and prohibits disclosure. Illinois, Texas, Washington, Arkansas, New York, and California have punitive laws.

ESF-17

- **Qualifying Entities:** State political subdivisions and critical infrastructure (*GOHSEP review*).
- **Permissive Services:** ESF-17 services are ***NOT compulsory;*** ESF-17 services may be terminated at any time by victim.
- **Requirements to Receive ESF-17 Services (not exclusive list):**
  - Executed Memorandum of Agreement containing standard T&Cs. Examples: liability waiver and indemnity for ESF-17 agencies and personnel (including contractors and volunteers), duty of confidentiality, public disclosure limitations, subrogation in favor of ESF-17, defined scope of work, disclaimer.
  - On-site working space for ESF-17 personnel during term of services (require internet connectivity, sufficient air conditioning, access badges, and desk-space at victim site).
  - ESF-17 services are dependent on ESF-17's available resources ("first-come, first serve" basis).
  - La. R.S. Title 29 Immunity
  - Submitted WebEOC request by Victim through GOHSEP.

Leadership: Office of Technology Services & Louisiana National Guard.

Formal Establishment: JBE Executive Order 19-12 to conduct cyber incident response and management.

Multi-Agency Partnership: OTS (primary agency), Louisiana Military Department (primary agency), Governor's Office of Homeland Security and Emergency Preparedness ("GOHSEP"), and Louisiana State Police Cyber Crime Unit ("CCU").

Response Statistics: *constantly changing…*

- >100 incident responses (between 2019-present day)
- Almost 5000 servers
- 73,000+ endpoints
- All 64 parishes

ESF-17

No Cost Support: CCU performs in-depth forensic analysis at no cost to the victim.

- Cannot remediate issue without forensics. CCU enjoys relationships with cyber forces from United States Secret Service, Federal Bureau of Investigation, and Department of Homeland Security.

Limited Interruption to Operations: *GENERALLY,* CCU takes memory sample and conducts analysis in CCU laboratory, minimally impacting operations.

- ESF-17 Personnel wear normal civilian clothes (not uniforms), blending into surroundings to avoid alarm.

Liability Mitigation: Protected by the Louisiana Cybersecurity Information Sharing Act (La. R.S. 51:2101 *et seq.)* and federal Cybersecurity Information Sharing Act (6 U.S.C. 1501 *et seq.)*

- Legal benefits:
  - Protection from liability when monitoring own network and sharing cyber threats or defensive measures with "appropriate entities."
  - Information shared cannot be used for anti-trust violations and information cannot be used to regulate or take enforcement actions against the entity (excepting crimes).
  - Entity maintains all legal privileges and all information shared is exempt from FOIA/State Public Records Act.
- Appropriate Entities: Louisiana's Fusion Center, Louisiana AG's office, and LSP along with DHS, DOE,DOJ, DOD…
- Scrub PII prior to sharing if possible.

QUESTIONS?

Sarah W. Anderson
225.615.0810
Sarah.Anderson@la.gov / Sarah@Alexandersides.com