

# **LAWS**

## **Legal and regulatory issues**

Dr. Shahzada Khurram

# Legal and regulatory issues

As IT Security Professionals we need to understand that laws and regulations have a huge influence on how we work.

We need to know some of them and understand how the rest work.

There are 4 types of laws covered on the exam and important to your job as an IT Security Professional.

## ○ **Criminal Law:**

- "Society" is the victim and proof must be "Beyond a reasonable doubt".
- Incarceration, death and financial fines to "Punish and deter".

## ○ **Civil Law** (Tort Law):

- Individuals, groups or organizations are the victims and proof must be "the majority of proof".
- Financial fines to "Compensate the victim(s)".

## ○ **Administrative Law** (Regulatory Law):

- Laws enacted by government agencies (FDA Laws, HIPAA, FAA Laws etc.) Proof "More likely than not".

## ○ **Private Regulations:**

- Compliance is required by contract (For instance PCI-DSS).

## ○ Liability:

If the question is who is ULTIMATELY liable, the answer is Senior Leadership. This does not mean you are not liable; you may be, that depends on Due Care. Who is held accountable, who is to blame, who should pay?

## ○ Due Diligence and Due Care:

❑ **Due Diligence** – The research to build the IT Security architecture of your organization. Best practices and common protection mechanisms. Research of new systems before implementing.

❑ **Due Care** – Prudent person rule – What would a prudent person do in this situation?

- Implementing the IT Security architecture, keep systems patched. If compromised: fix the issue, notify affected users (Follow the Security Policies to the letter).

○ **Negligence** (and gross negligence) is the opposite of Due Care.

○ If a system under your control is compromised and you can prove you did your Due Care, you are most likely not liable.

○ If a system under your control is compromised and you did NOT perform Due Care, you are most likely liable

# Evidence

How you obtain and handle evidence is VERY important.

## ○ Types of evidence:

- **Real Evidence:** Tangible and physical objects in IT Security: Hard disks, USB drives – NOT the data on them.
- **Direct Evidence:** Testimony from a firsthand witness, what they experienced with their 5 senses.
- **Circumstantial Evidence:** Evidence to support circumstances for a point or other evidence.
- **Collaborative Evidence:** Supports facts or elements of the case: not a fact on its own but support other facts.
- **Hearsay:** Not first-hand knowledge – normally inadmissible in a case.
  - Computer-generated records and with that log files were considered hearsay, but case law and updates to the Federal Rule of Evidence have changed that. Rule 803 provides for the admissibility of a record or report that was “made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation.”

- **Best Evidence Rule** – The courts prefer the best evidence possible.
  - Evidence should be accurate, complete, relevant, authentic, and convincing.
- **Secondary Evidence** – This is common in cases involving IT.
  - Logs and documents from the systems are considered secondary evidence.
- **Evidence Integrity** – It is vital that the evidence's integrity cannot be questioned.
  - We do this with hashes. Any forensics is done on copies and never the originals.
  - We check hash on both original and copy before and after the forensics.
- **Chain of Custody** – This is done to prove the integrity of the data; that no tampering was done.
  - Who handled it?
  - When did they handle it?
  - What did they do with it?
  - Where did they handle it?



# Reasonable Searches:

## Reasonable Searches:

- The Fourth Amendment to the United States Constitution protects citizens from unreasonable search and seizure by the government.
- In all cases, the court will determine if evidence was obtained legally. If not, it is inadmissible in court.
- Exigent circumstances apply if there is an immediate threat to human life or of evidence destruction.
  - This will later be decided by a court if it was justified.
  - Only applies to law enforcement and those operating under the “color of law” – Title 18. U.S.C. Section 242 – Deprivation of Rights Under the Color of Law.
- Your organization needs to be very careful when ensuring that employees are made aware in advance that their actions are monitored, that their equipment, and maybe even personal belongings, can be subjected to searches.
  - Notifications like that should only be made if your organization has security policies in place for it, and it must take into account the privacy laws in your county/state/country.

# Entrapment and Enticement

- **Entrapment** (Illegal and unethical): When someone is persuaded to commit a crime they had no intention of committing and is then charged with it.
  - Openly advertising sensitive data and then charging people when they access them.
  - Entrapment is a solid legal defense.
- **Enticement** (Legal and ethical): Making committing a crime more enticing, but the person has already broken the law or at least has decided to do so. Honeypots can be a good way to use Enticement.
  - Have open ports or services on a server that can be attacked.
  - Enticement is not a valid defense.
- If there is a gray area in some cases between Entrapment and Enticement, it is ultimately up to the jury to decide which one it was.
- Check with your legal department before using honeypots. They pose both legal and practical risks

# GDPR

## GDPR (General Data Protection Regulation):

- GDPR is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).
- It does **not** matter where we are based, if we have customers in EU/EEA we have to adhere to the GDPR.
- Violators of the GDPR may be fined up to €20 million or up to 4% of the annual worldwide turnover of the preceding financial year in case of an enterprise, whichever is greater.
- Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so.

○ **Restrictions:** Lawful interception, national security, military, police, justice.

○ **Personal data** covers a variety of data types including: Names, Email Addresses, Addresses, unsubscribe confirmation URLs that contain email and/or names, IP Addresses



# GDPR (General Data Protection Regulation)

- **Restrictions:** Lawful interception, national security, military, police, justice.
- **Right to access:** Data controllers must be able to provide a free copy of an individual's data if requested.
- **Right to erasure:** All users have a 'right to be forgotten'.
- **Data portability:** All users will be able to request access to their data 'in an electronic format'.
- **Data breach notification:** Users and data controllers must be notified of data breaches within 72 hours.
- **Privacy by design:** When designing data processes, care must be taken to ensure personal data is secure. Companies must ensure that only data is 'absolutely necessary for the completion of duties'.
- **Data protection officers:** Companies whose activities involve data processing and monitoring must appoint a data protection officer.



Thank you