Developments in CyberSecurity Law

presented by

UDALL
LAW FIRM LLP

TUCSON - PHOENIX

www.udalllaw.com

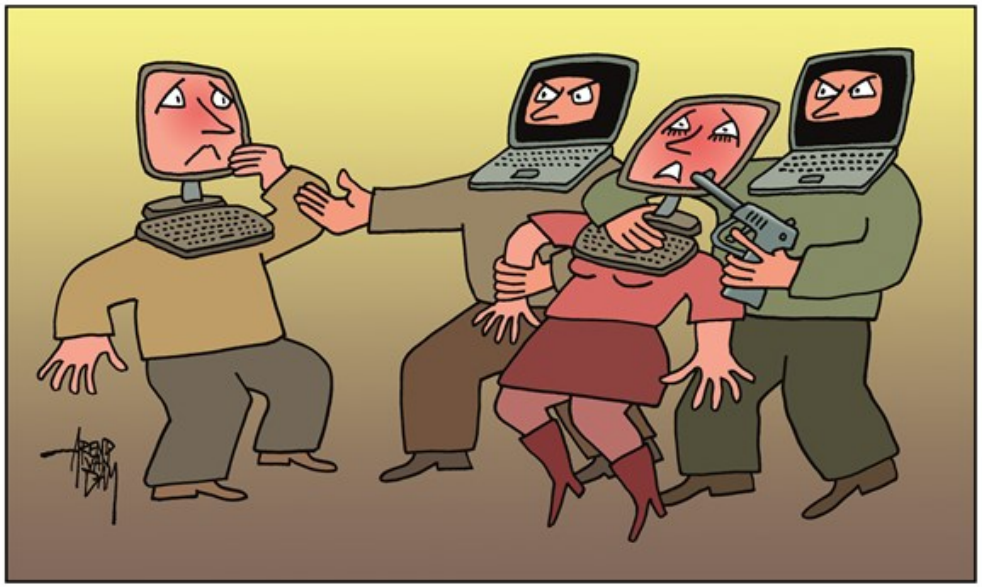
Security Breaches
&
Security Requirements

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Security Breaches

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Criminal Conduct

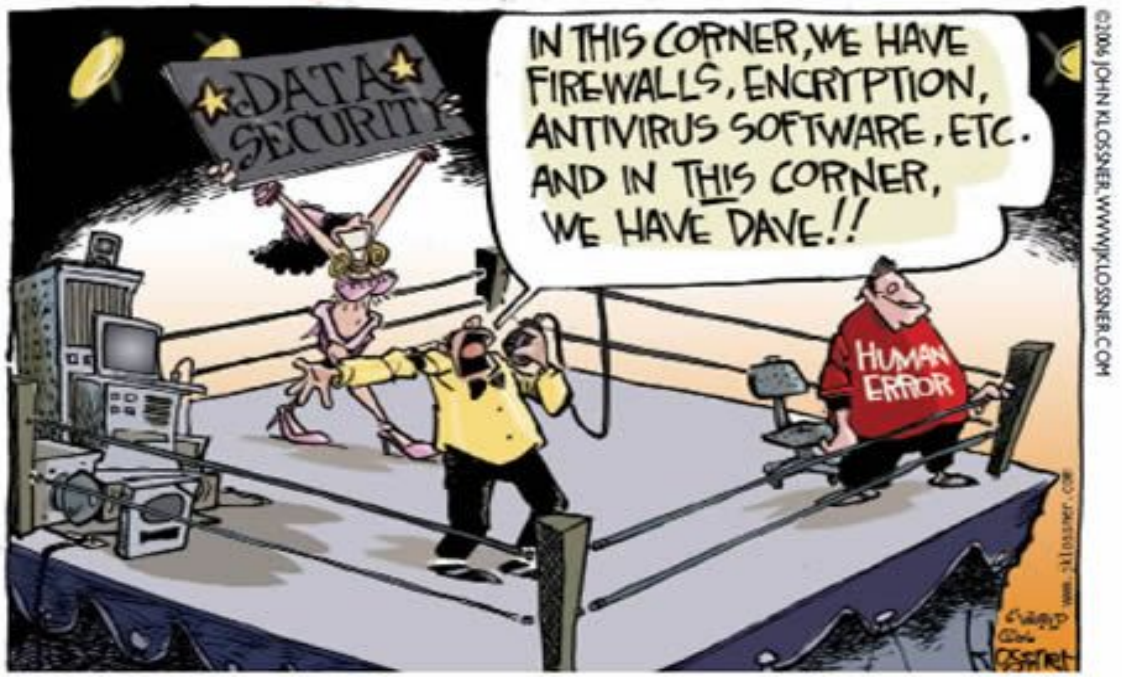


RANSOMWARE

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

-computer viruses (ransomware)
-physical theft
    -server, laptops, flash drives
-electronic theft of data

Human Error



UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Who Does it Affect?

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Financial & Legal Implications

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Financial

- Halts your business
- Forensic IT experts
- Ransom
- Customer Notification
- Credit Monitoring
- Lawyers
- Time

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Legal

- Arizona Law
- HIPAA/HITECH
- FTC Enforcement
- Common Law/Negligence Liability
- International Law-GDPR
- Other States' Laws

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Arizona Law
A.R.S. §18-552

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Applies to any person or business who conducts business in Arizona and owns or maintains unencrypted or unredacted computerized personal information

Personal information includes:
Name +
SSN
Driver's License Number
Medical Information
Username
Email Address
Financial Account/CC Number
Health Insurance Number
Passport Number

In case of a breach:

-Notification of affected individuals within 45 days
-If >1000 affected, notification to consumer reporting agencies and AG
-Civil Penalties

Federal Law: HIPAA/HITECH

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Privacy & Security Regulations

-applies to covered entities
-protects PHI
-requires reasonable safeguards to secure PHI (physical, administrative, and technical)

Health Information Technology for Economic and Clinical Health Act ("HITECH")

- Includes breach notification
- Gives power to state attorney generals
- Increased fines
- Makes "business associates" subject to enforcement (audits and fines)

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Who is a Business Associate?

A person or entity that creates, receives, maintains or transmits protected health information to perform certain functions or activities on behalf of a covered entity.

Requirements for Business Associates

-must comply with privacy rules
-must notify covered entity in case of breach
-business associate agreement
-subcontractor agreement
-must perform a risk analysis
-must implement security safeguards
-adopt security policies
-train personnel
-can be audited

FTC ENFORCEMENT

- No comprehensive federal data security law nor explicit mandate for FTC to police data security.
- Patchwork of state and industry-specific data security and privacy laws allow FTC to bootstrap enforcement through “deceptive trade practices” laws.
- Few explicit security requirements, the prevalent US model is “market driven” security.
- Substantive security requirements can be imposed through settlement agreements.

Examples of State and Industry-Specific Laws

- **California Online Privacy Protection Act (CalOPPA)** – requires a privacy policy for any website or online service that collects personally identifiable information about California residents.

- **Gramm-Leach-Bliley Act** – requires a privacy policy for companies "significantly engaged" in the financial industry.

- **Children's Online Privacy Protection Act** – requires a privacy policy for any website or online service that collects information about, or targets children under the age of 13.

Privacy Policies

- Market-driven approach to privacy/security regulation – inform the data subjects about uses and safeguards, let them decide whether to share data.

- Typical contents of privacy policy:
  - What information is collected
  - How information is collected
  - How information is stored and protected
  - How information is used
  - How information is distributed
  - What rights customers have with respect to the information

Negligence Liability

- Common law negligence: duty, breach, causation, damages.
- Is there a duty to safeguard data?
- Varying results in the courts, no broad ranging precedents.

Example Case - Ashley Madison

- Online dating service targeted towards married individuals.
- Based in Canada, but advertised services to US customers and had almost $50 million in annual revenue from US customers.
- Advertised as “100% Secure”, “Certified Zero Risk” and “Completely Anonymous”.
- Allowed customers to pay $19 for a “Full Delete”. Fine print indicated that some information would be retained.
- Malicious actor accessed the data and posted it publicly.
- FTC pursued charges under deceptive trade practices laws for misrepresentations about the security of information and the information retained.
- Settlement imposed $8 million penalty and data security program and audits.

Example Case - Equifax

- Personal information for 143 million Americans breached, including name, DOB, SSN, contact info, etc.
- Equifax failed to disclose breach for several months after it was discovered.
- No significant FTC or CFPB enforcement.
- Banking regulators in several states entered into a consent order with Equifax requiring improved security infrastructure, auditing and reporting.
- Class action lawsuits ongoing, assert general negligence.
- Some amount of small-claims suits, with varying success.
- Equifax argues “no duty of care to safeguard personal information” and no actual damages.
- Only significant charges were for insider trading.
- Significant negative publicity, however the lasting impact is unclear.

Example Case - Delta

- Delta Airlines created a mobile app which did not contain a privacy policy.
- California asserted a violation of CalOPPA, potential penalties of up to $2,500 for each download of the app by a California resident.
- Delta was selected as the “test case” for CalOPPA prosecution.
- Federal judge dismissed California’s complaint on federal preemption grounds – the Airline Deregulation Act preempted state regulation of the airline’s activities.
- Seen as a large defeat for the effectiveness of CalOPPA, but it is unclear how many other business can succeed on similar preemption grounds.
- Delta now includes a privacy policy on its app, despite the court’s ruling.

International Law

General Data Protection Regulation (GDPR)

- Applies to all companies offering goods or services to "Data Subjects" of the EU:
  - Physically conducting business in EU
  - Targeting EU customers
- Contains affirmative requirements to safeguard data – companies must do a risk assessment and provide a "reasonable" level of protection.
- Requires disclosure of the data collected and how it is used; requires "opt-in".
- Requires breach notifications.
- Grants a right to access your data.
- Grants a "right to be forgotten".

New State Laws

- California Consumer Privacy Act
  - Similar to GDPR, but focuses more on privacy than data security.
  - Requires equal service and price for opt-outs
  - Goes into effect Jan 1, 2020
- New York SHIELD Act
  - Focuses more on security than other similar laws.
  - Gives clearer picture of security requirements:
    - designating a data security officer;
    - identifying "reasonably foreseeable" risks;
    - selecting vendors that maintain appropriate safeguards;
    - detecting, preventing and responding to attacks and system failures.
  - Give protection to companies that get independently certified for certain cybersecurity standards.

Takeaways

- Err on the side of having a privacy policy, even in the absence of a clear mandate.
- If you have a privacy policy, follow it.
- The fine print wont save you.
- Be proactive about security.
- Limit the amount of data collected/stored.

QUESTIONS?

"You may want to look into getting a better cybersecurity system. I don't think that sign will be enough."

UDALL
LAW FIRM LLP
TUCSON - PHOENIX

Michele G. Thompson
mthompson@udalllaw.com
(520) 623-4353

Evan Manning
emanning@udalllaw.com
(520) 623-4353

UDALL
LAW FIRM LLP
TUCSON - PHOENIX