Breakfast Bites

WHAT'S THE WORST THAT CAN HAPPEN? PROTECTING EMPLOYERS WITH A COMPREHENSIVE DATA PROTECTION PLAN

Jordan B. Segal, Esq.

Maddin Hauser
Attorneys and Counselors

Maddin, Hauser, Roth & Heller, P.C.
28400 Northwestern Hwy. Southfield, MI 48034
p (248) 354-4030 f (248) 354-1422 maddinhauser.com

Jordan B. Segal

Associate

p (248) 359-7539

f (248) 359-7579

jsegal@maddinhauser.com

Maddin Hauser

Attorneys and Counselors

Maddin, Hauser, Roth & Heller, P.C.

28400 Northwestern Hwy. Southfield, MI 48034

p (248) 354-4030 f (248) 354-1422 maddinhauser.com

Overview

- Current Trends, and Legal Risks
- Planning for a Breach
  - Outline of a data security plan
  - Legal tools at your disposal to protect your data
- Recent Legal Developments
  - Legislation
  - Lessons from the Courts
  - Government initiatives

THE GREAT CYBER-CRIME WAVE OF 2020-2022

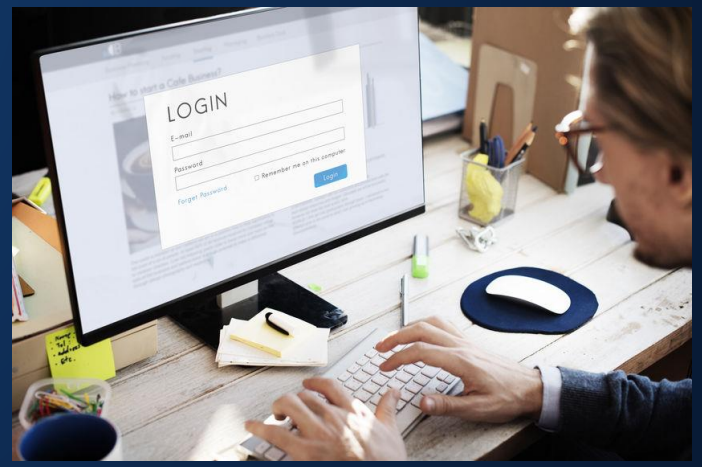
- The Scope of Cyber Crime Activity
  - Data breaches resulted in 36 billion records being exposed in the first three quarters of 2020. Despite this, the number of publicly reported breaches decreased by 51% compared to the same time last year.
  - The use of malware increased by 358% through 2020, and ransomware to one study. July 2020 alone saw a 653% increase in malicious activity compared to the same month in 2019.
  - More than 90% of healthcare organizations suffered at least one cybersecurity breach in the previous three years, according to the U.S. Healthcare Cybersecurity Market 2020 report.

THE GREAT CYBER-CRIME WAVE OF 2020-2022

- The Cost of Cyber Crime
  - Cyber crime costs organizations $2.9 million every minute, and major businesses lose $25 per minute as a result of data breaches.
  - According to research by IBM, the average attack costs $3.86 million.
  - The U.S. has the world's highest data breach costs, with the average attack costing $8.6 million, according to IBM's Cost of a Data Breach report.

THE GREAT CYBER-CRIME WAVE OF 2020-2022

- The Threat Within
  - According to Verizon's 2015 Data Breach Investigations Report, about 50 percent of all security incidents are caused by people inside an organization.
    - 30 percent of all cases are due to worker negligence like delivering sensitive information to the wrong recipient or the insecure disposal of personal and medical data.
    - 20 percent are insider misuse events, where employees could be stealing and/or profiting from company-owned or protected information.

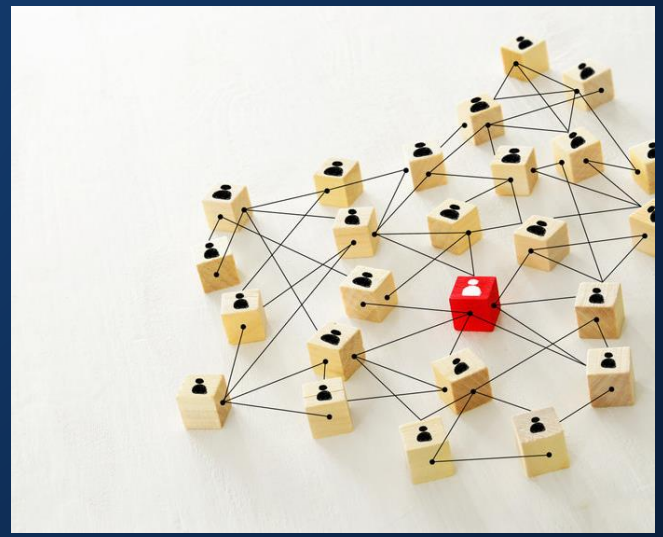


LEGAL RISKS

- Notification Laws
- Industry-Specific Regulations
- Direct Legal Liability

LEGAL RISKS – NOTIFICATION LAWS

- All 50 states and the District of Columbia require businesses to notify individuals of breaches of information involving personally identifiable information.
- For each jurisdiction, be aware of:
  - What is a “breach” (and is a potential breach enough to trigger notice?)
  - Threshold of residents affected for notification and what notice must say.
  - Who must be notified? (consumer, Attorney General’s office, others?)
  - Deadlines.
  - Safe harbors?



LEGAL RISKS – INDUSTRY SPECIFIC REGULATIONS

- *HIPAA* and *HITECH*: Healthcare
- *Gramm Leach Bliley Act*: Consumer information held by financial institutions
- *Fair Credit Reporting Act*: Credit data
- See also certain State laws: e.g. the *Michigan Data Security Act*

LEGAL RISKS

- Direct Legal Liability for a Data Breach is Rare
  - Causation is hard to prove.
  - Damages are hard to establish.
  - What a “reasonable level of data protection” is not yet commonly agreed upon.

LEGAL RISKS

- But, see *Dittman v UPMC*, 196 A3d 1036 (PA 2018) (employer held liable for the damages suffered by its employees following a hack of its HR systems).
- An Employer is under a “legal obligation to exercise reasonable care to safeguard its employees’ sensitive personal information stored by the employer on an internet-accessible computer system”

BREACH PLANNING

- Lessons from HIPAA/HITECH (not all will apply):
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Organizational safeguards
  - Policies, procedures and documentation

BREACH PLANNING

- Assemble your Data Breach Response Team
  - Legal
  - Information Technology
  - Forensics
  - Operations
  - Human Resources
  - Investor Relations
  - Management

LEGAL TOOLS TO PROTECT DATA

- Nondisclosure Agreements and Noncompetition Agreements
  - Limit the use of proprietary data by good faith operators.
  - Require that data accessed by third parties is kept securely.
  - Adds accountability for bad actors.
  - Provide a remedy against identifiable individuals.

NONDISCLOSURE AGREEMENTS

- Define “Proprietary Data” or “Confidential Information”
  - As broad a definition as required under the circumstances.
  - Include flexibility to mark items as “confidential.”
  - Include “notes, memorandum, analyses etc.” that is based on confidential information.
  - Exclude material that is already in the public domain.

NONDISCLOSURE AGREEMENTS

- Protection of “Confidential Information”
  - Term: during the agreement and for a period of time thereafter:
    - Think about how long before your data goes “stale”
  - Who gets to be in the “Circle of Trust”?
    - Experts (Accountants, Attorneys, etc.)?
    - Employees?
    - Must these people sign before they get access?
  - Level of Protection
    - Standard language: use the same level of protection as for one’s own data
    - Is this sufficient?

NONDISCLOSURE AGREEMENTS

- Protection of “Confidential Information”
  - For which uses may the recipient use data
    - Any use?
    - A particular project of transaction?
  - Ownership and Return of Data
    - YOU WERE, ARE, AND WILL ALWAYS BE THE OWNER OF THE DATA
    - Return of data upon request? Automatically?
    - Destroy all copies
    - Certification (under oath)?

NONCOMPETITION AGREEMENTS

NONCOMPETITION AGREEMENTS

- An agreement or clause in a contract specifying that an employee must not enter into competition with an employer after the employment period is over.
- A carefully crafted noncompete can help prevent employees from being able to “sell” information for a new job at a competitor
- Note: rules vary by jurisdiction

NONCOMPETITION AGREEMENTS

- Limited as to Scope of Employment
  - Define “competition”
  - List competitors
  - List “hands-off” customers or all customers
  - Vendors and Suppliers
  - Other special relationships
- You cannot wholesale prevent someone from working in their chosen profession

NONCOMPETITION AGREEMENTS

- Reasonable Geographic Restriction
  - Radius area around office/factory/facility?
  - Market area?
  - Jurisdiction?
  - National?
- What is “reasonable” will vary based on the individual circumstances of the business and its industry

NONCOMPETITION AGREEMENTS

- Reasonable Time Limit
  - 1-3 years is generally enforceable on a sliding scale with other limitations.
  - Include a provision that extends the restricted period during time which employee is in breach.
- The Court may “blue-pencil” the terms if the noncompete is overbroad or too harsh.

LEGAL DEVELOPMENTS

DEFEND TRADE SECRETS ACT OF 2016

LEGAL DEVELOPMENTS

- DEFEND TRADE SECRETS ACT 18 USC 1836
  - The DTSA provides a private civil cause of action for victims of trade secret theft where a trade secret has been misappropriated, and requires that the misappropriated trade secret is related to a product or service used in, or intended for use in, interstate commerce.
  - Provides federal jurisdiction for trade secret theft, which was previously a state-law offense.
  - Enhanced damages and attorneys fees.
  - Easier access to national court systems, instead of local state courts.

LEGAL DEVELOPMENTS

DEFEND TRADE SECRETS ACT
18 USC 1836

- The *ex parte* seizure remedy is one of the most potent weapons the DTSA affords to trade secret holders. It empowers a court to issue an order to allow law enforcement to seize stolen trade secrets without hearing the opposing party's argument.
- *Whistle-Blower Immunity*. The DTSA also includes an "immunity" provision, which exempts whistleblowers from liability for any trade secret disclosure made "solely for the purpose of reporting or investigating a suspected violation of law" to attorneys or government officials. Employers ***must*** provide notices to their employees about the availability of this "immunity, or lose certain benefits of the DTSA.

LEGAL DEVELOPMENTS

- *Van Buren v. United States*
  - The Supreme Court severely restricted the definition of "exceeding authorized access" to "those who obtain information from particular areas in the computer—such as files, folders, or databases—to which their computer access does not extend. It does not cover those who . . . have improper motives for obtaining information that is otherwise available to them."
- Consider adopting a "Need-To-Know Only" data structure

Breakfast Bites

QUESTIONS

Maddin Hauser
Attorneys and Counselors

Maddin, Hauser, Roth & Heller, P.C.
28400 Northwestern Hwy. Southfield, MI 48034
p (248) 354-4030 f (248) 354-1422 maddinhauser.com

Breakfast Bites

THANK YOU

Jordan B. Segal
Associate

p (248) 359-7539

f (248) 359-7579

jsegal@maddinhauser.com

Maddin Hauser
Attorneys and Counselors

Maddin, Hauser, Roth & Heller, P.C.
28400 Northwestern Hwy. Southfield, MI 48034
p (248) 354-4030 f (248) 354-1422 maddinhauser.com