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

By Jordan B. Segal

I. CURRENT TRENDS AND LEGAL RISKS

A. The Great Cyber Crime Wave of 2020-2022

1. Data

a. 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.[1]

b. 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.[2]

c. 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.

2. The Cost of Cyber Crime

a. Cyber-crime costs organizations $2.9 million every minute, and major businesses lose $25 per minute as a result of data breaches.[3]

b. According to research by IBM, the average attack costs $3.86 million.[4]

c. 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.[5]

---

[1] Whitepaper, Risk Based Security 202 Q3 Data Breach Report https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf

[2] Cisco 2021 Cybersecurity Threat Report, https://umbrella.cisco.com/info/2021-cyber-security-threat.html

[3] Accenture Security, The Cost of Cybercrime, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[4] https://www.ibm.com/security/data-breach

[5] *Id.*

3. The Threat Within

a. According to Verizon's 2015 Data Breach Investigations Report, about 50 percent of all security incidents are caused by people inside an organization.[6]

b. 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.[7]

c. 20 percent are insider misuse events, where employees could be stealing and/or profiting from company-owned or protected information.[8]

B. Legal Risks

1. Notification Laws[9]

2. Industry Specific Regulations

a. HIPAA[10]/HITECH[11]

b. Gramm Leach Bliley[12]

c. Fair Credit Reporting Act[13]

d. Michigan Data Security Act (see also: CPRA, GDPR, etc).

3. Direct legal liability[14]

II. PLANNING FOR A BREACH

A. Lessons from HIPAA

---

[6] https://www.verizon.com/business/resources/reports/dbir/

[7] *Id.*

[8] *Id.*

[9] https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx; Mich. Comp. Laws § 445.63, 445.72; Mich. Comp. Laws § 445.63, 445.72

[10] 42 USC 1302

[11] 42 USC 17935

[12] 15 USC 6802

[13] 15 USC 1681

[14] *Dittman v UPMC*, 196 A3d 1036 (PA 2018)

1. Administrative safeguards might entail hiring a vendor to perform a cyber risk analysis, or a long-term risk management program to reduce IT system risks and vulnerabilities.

2. Physical safeguards are the actual, real world (opposed to online or electronic) barriers put in place to protect data; these might include locked server rooms and other physical measures intended to keep physical access to servers or other data storage to a minimum.

3. Technical safeguards include firewalls, anti-malware scanning, and other electronic mechanisms designed to keep data secure.

4. Organization safeguards address a company's relationships with its vendors and may require best practices such as indemnification for outside data breaches, warranties that vendors will use industry standard encryption protocols, and other contractual measures.

5. Policies, procedures, and documentation mean having a written data breach plan, data backup plans, and other set procedures for staff to follow in the event of a cyberattack. This can and should also include data security training for employees that is tailored to your specific risk profile.

B. Assemble your Data Breach Response Team:

5. Legal

6. Information Technology

7. Forensics

8. Operations

9. Human Resources

10. Investor Relations

11. Management

C. Nondisclosure Agreements

1. Define Proprietary Data

2. Set Parameters for protection of Data:

a. Term

b. To whom may information be disclosed

c. How much protection is required

d. Data Use restrictions

e. Ownership and return of data

D. Noncompetition Agreements

1. Limits as to Scope of Employment

2. Reasonable Geographic restrictions

3. Reasonable time limitations

III. RECENT LEGAL DEVELOPMENTS

A. Defend Trade Secrets Act of 2016

1. 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.

2. Provides federal jurisdiction for trade secret theft, which was previously a state-law offense.

3. Enhanced damages and attorneys' fees.

4. Easier access to national court systems, instead of local state courts.

5. 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.

6. *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.

7. Employers ***must*** provide notices to their employees about the availability of this "immunity, or lose certain benefits of the DTSA

B. Van Buren v United States

1. The Computer Fraud and Abuse Act (CFAA) is an anti-hacking statute making it illegal "to access a computer without authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to so obtain or alter."

2. Violations of the statute may trigger criminal prosecution or civil litigation by private parties. On June 3, 2021, in Van Buren v. United States, a 6-3 majority of the U.S. Supreme Court adopted

a restrictive view of the CFAA, making it more difficult for employers to invoke the statute in cases arising from the theft of trade secrets.

3. The CFAA (codified at 18 U.S.C. § 1030) was enacted in 1986, based on a number of hacking incidents as well as -- allegedly -- Reagan White House viewings of the movie "War Games." It was originally intended to deter hacking into government computers, financial institution networks, and other "protected computers."

4. Employers typically allege CFAA violations after, for example, an employee downloads or emails confidential information to benefit a competitor. In these types of cases, the employer may file a CFAA claim because the CFAA provides a basis for subject-matter jurisdiction in federal court, triggers the possibility of enhanced sanctions, and arguably provides a means of protecting confidential information that does not rise to the level of a "trade secret."

5. An oft-litigated question is whether an employee provided with unlimited access to the employer's computer system, but who uses that access to use information for purposes beyond the employee's authority ("ultra vires" purposes), has accessed the employer's computer "without authorization" or in a manner that "exceed[ed] authorized access" in violation of the CFAA.

6. In Van Buren, the Supreme Court took a narrow view, holding that the CFAA "covers 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." Van Buren definitively prevents an employer from asserting a CFAA claim against an employee provided with unlimited access to the employer's computer system, but who uses that access to use information for ultra vires purposes.

7. As a practical matter, Van Buren narrows employers' ability to use the CFAA as a basis for federal subject-matter jurisdiction and narrows remedies available to employers in the "disloyal employee" scenario. There are, however, two ways employers can limit Van Buren's impact.

8. First, employers may craft computer-use policies and procedures expressly forbidding and preventing employees from accessing particular files, folders, and databases. An employee who circumvents such a prohibition likely will have violated the CFAA even under Van Buren's narrow reading of the statute, and an employer may proceed civilly against that employee under the CFAA. Second, in a "disloyal employee" scenario involving the theft of trade secrets, an employer should consider filing a claim for violation of the Defense of Trade Secrets Act, which will provide a basis for federal subject-matter jurisdiction and lessen the need to rely solely on the CFAA for that purpose.

9. Employers are also encouraged to work with their employment law counsel to ensure they have proper security protocols and restrictive covenant agreements in place to protect their proprietary information.