UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

36th Annual School Law Conference

February 22, 24, 26, 2021
Live Webcast

Ransomware Attacks: Not If, But When

Kimberly Celeste Gordy

Examples of Reasonable Security Measures

- **Align to a security framework** – such as NIST CSF. Many of the other items listed below are identified as components of one of these security frameworks.
- **Do a regular risk assessment** – identify critical assets, threats, and vulnerabilities. Use assessment to prioritize cybersecurity roadmap/maturity plans.
- **Know your environment** – if you do not know what devices you have, you cannot defend them (e.g., avoids scenarios where you deploy an endpoint tool but it does not get provisioned on every device. The unknown devices will be the first compromised).
- **Know what data you have and where it resides** – if you do not know what data you have and where it resides, you are not likely to implement appropriate measures (or even know when there is unauthorized access to it). A data inventory is also helpful to segregate student information that may be stored locally.
- **Multifactor authentication** – enable MFA where you can, especially for Office 365 (and disable backwards compatible apps that do not support MFA/modern authentication) and any other cloud-based application where logging in provides access to sensitive data (e.g., your student database, payroll services like ADP – apply MFA at least for HR admin users).
- **Manage cloud assets** – address access rights for cloud resources, including Google Workspace, Dropbox, Google Docs (make sure that they are not set to public access where anyone that knows the url can see what is in the bucket).
- **Endpoint security** – deploy an endpoint tool that goes beyond signature-based AV detection. Examples are FireEye's HX agent, CrowdStrike's Falcon, Carbon Black, Tanium, or Cylance.
- **Encryption** – encrypt portable devices (e.g., laptops, USB drives), sensitive data at rest (e.g., Student records, payroll, SSNs), and passwords for online accounts (do not just hash).
- **Patch management** – use a tool for patching and evaluate patching cycle.
- **Logging and log monitoring** – If possible, use a SIEM and have a SOC (internal or outsourced) to provide 24/7 monitoring of logs and alerts. Talk to security firm that does forensic investigations about log retention and details to log (this identifies evidence sources that enable them to be more precise in their investigation). Be sure to turn on auto logging.
- **Phishing** – use an email filter to reduce the number of phishing emails that get through (e.g., Proofpoint, Mimecast, FireEye's ETP)
- **Security awareness training** – design and implement a program that teaches staff about phishing and social engineering. Test phishing exercises are pretty common.
- **Continuity** – ransomware has become very problematic. Have good backups that are readily available and not stored on each host they are a backup of.
- **Effective Communication** – ensure you have a backup plan to communicate with parents if remote school is canceled.

Texas

Data Breach Notification Statute (Full Text)

V.T.C.A., Bus. & C. § 521.002
Definitions

(a) In this chapter:

(1) “Personal identifying information” means information that alone or in conjunction with other information identifies an individual, including an individual's:

(A) name, social security number, date of birth, or government-issued identification number;

(B) mother's maiden name;

(C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;

(D) unique electronic identification number, address, or routing code; and

(E) telecommunication access device as defined by Section 32.51, Penal Code.

(2) “Sensitive personal information” means, subject to Subsection (b):

(A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

(i) social security number;

(ii) driver's license number or government-issued identification number; or

(iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(B) information that identifies an individual and relates to:

(i) the physical or mental health or condition of the individual;

(ii) the provision of health care to the individual; or

(iii) payment for the provision of health care to the individual.

(3) “Victim” means a person whose identifying information is used by an unauthorized person.

(b) For purposes of this chapter, the term “sensitive personal information” does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

UT LAW CLE | THE UNIVERSITY OF TEXAS | TEXAS LAW

Also available as part of the eCourse
Ransomware Attacks: Not If, But When

First appeared as part of the conference materials for the
36th Annual School Law Conference session
"Ransomware Attacks: Not If, But When"