# Texas SB 820 - Cybersecurity Analysis and Plan

## The Analysis

**"We already have Firewalls, VPNs and anti-viruses/anti-malware so how are we at risk?"**

- Firewalls protect us from direct attacks over the internet by blocking everything but allowed traffic
- VPNs provide a secure way for our users to get to the network resources
- **Virus and malware scanners scan files looking for viruses and known malware**
  - To be able to **detect** malware and to be able to detect it, they have to have seen it before. The flow goes something like this:
    1. A virus/malware occurs in the world
    2. A security expert sees it and submits it to the Anti-virus publisher (e.g. McAfee)
    3. The publisher (e.g. McAfee) analyses the virus/malware and generates a 'signature', then updates the 'Signature file'
    4. The 'signature' file is downloaded by all the clients which allows them to detect and block the virus/malware
    5. This whole process can take several days, depending on how wide spread the attack is
  - **The risk is that there is an attack BEFORE a signature has been generated and distributed.** Here's a couple of ways that that can happen:
    - It's new malware (in 2017, a new malware specimen emerges every 4.2 seconds)
    - It's a targeted attack. The recent attacks on local governments in Texas are believed to be from a single source

**"How can we protect ourselves against malware that has never been seen before or even worse a targeted attack?"**

- Problem Analysis and assumptions:
  - 99.1% of all malware is targeting Windows
  - Ransomware is growing substantially
  - Recent varieties of Ransomware are encrypting network shares too
  - Malware can spread via the network
  - Malware, ransomware and even viruses are all programs
  - Legitimate programs installations rarely happen after initial computer set up
  - Installing programs require Administrator level access
    - Limited users cannot install programs due to Windows User Access Control
  - Malware doesn't get installed like normal programs, instead the malware program files are written to a temporary folder and ran directly from there

## The Plan:

- The problem with virus and malware scanners is that they need a ‘signature.’ We need a way to prevent malware without relying on a signature
- Since programs rarely get installed, especially by non-administrators, we should just block program files from being written to the hard drive. If the program files can’t be written to the computer, the operating system can’t find it to execute it

**“How can FileSure Defend and FileSure.cloud help?”**

- FileSure Defend and FileSure.Cloud can block file operations based on a ‘policy’/rules. For our needs, FileSure would block program files (.exe, .dll, .sys, .bat, etc…) from being written to the computer
  - This will prevent:
    - malware from being install from an infected email attachment (the most common technique)
    - malware from spreading over the network
    - if an exploit is found, most of the time it will attempt to download a more sophisticated program file….FileSure will block that
- FileSure is also a file auditing product so it will record system object changes and/or access to student files
- All activity is recorded and can be alerted and reported on

**“Is there a downside?”**

- Along with bad actors, FileSure Defend will block legitimate software installations and updates
  - We could look at this as a benefit since it will prevent people from installing without IT involvement
  - Microsoft and Google **updates will not be blocked**, but blocks others
  - There is a way to ‘pause’ protection to install legitimate software and updates
  - The ability to pause protection is controlled by the account owner (e.g. us)