Cybersecurity Threats for Law Firms

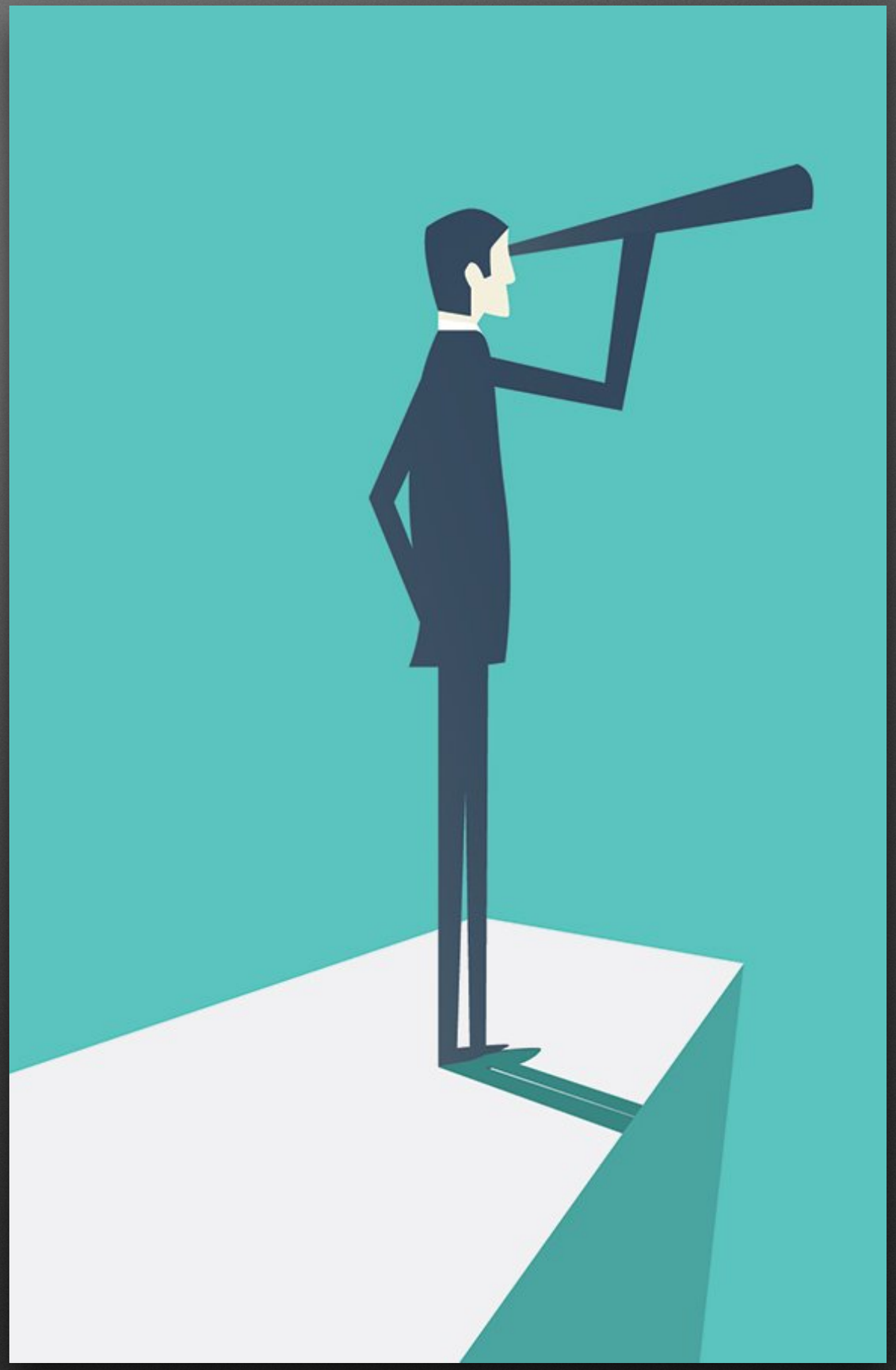
Ronald L. Chichester

Annual Meeting of the State Bar of Texas

Austin, Texas

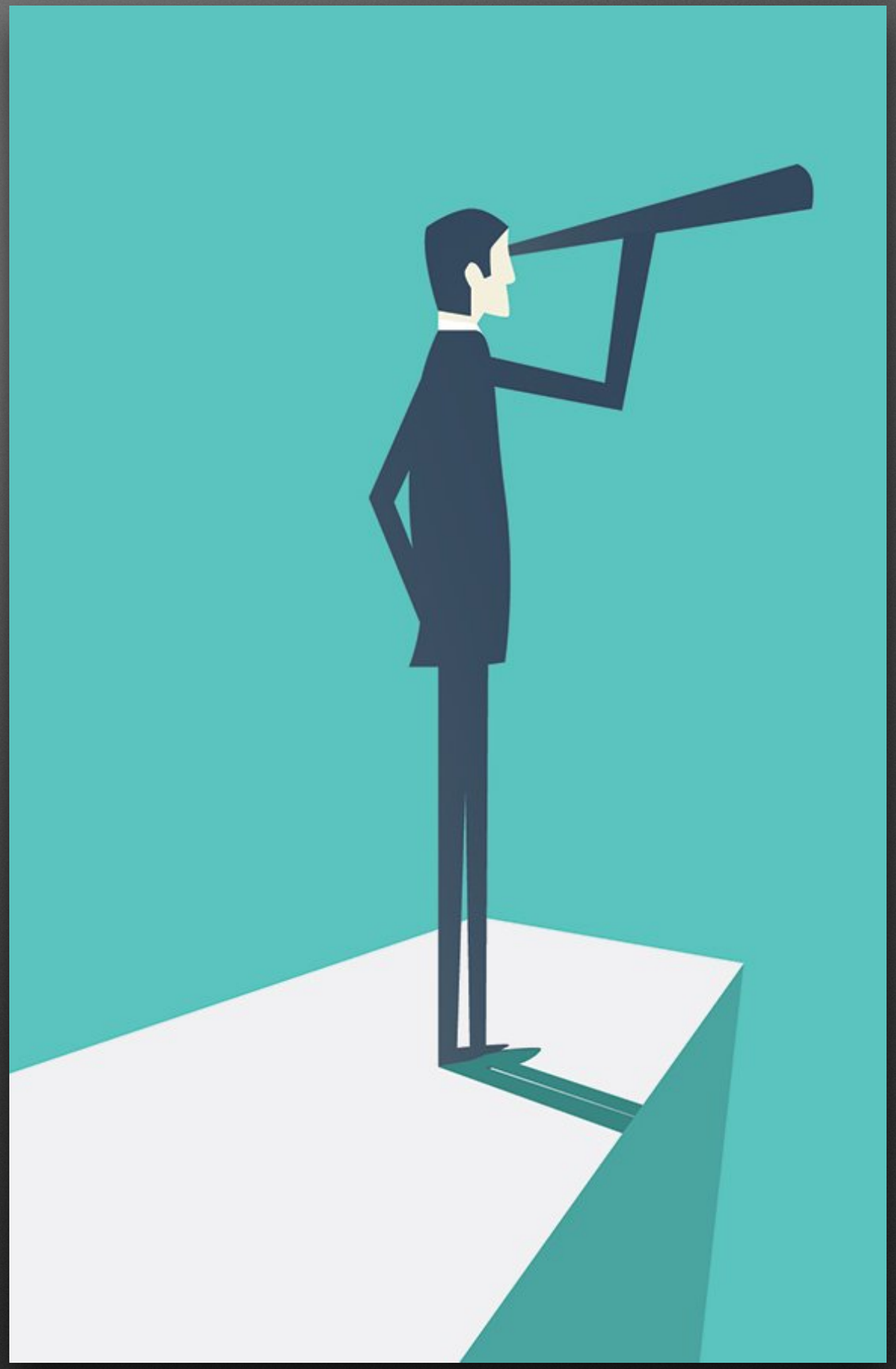
June 13-14, 2019

Overview



Overview

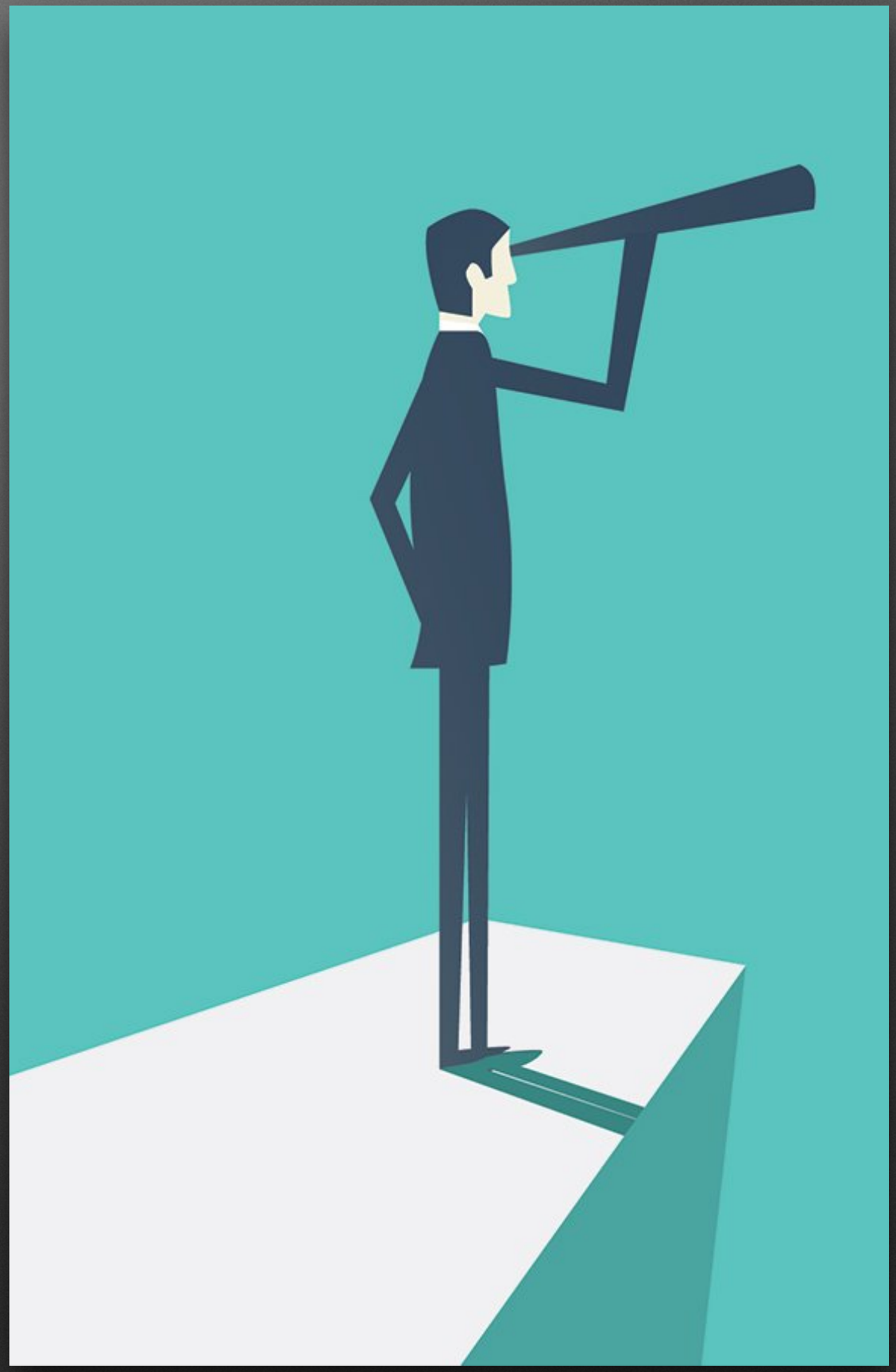
The Bombshell



Overview

The Bombshell

The Bad News

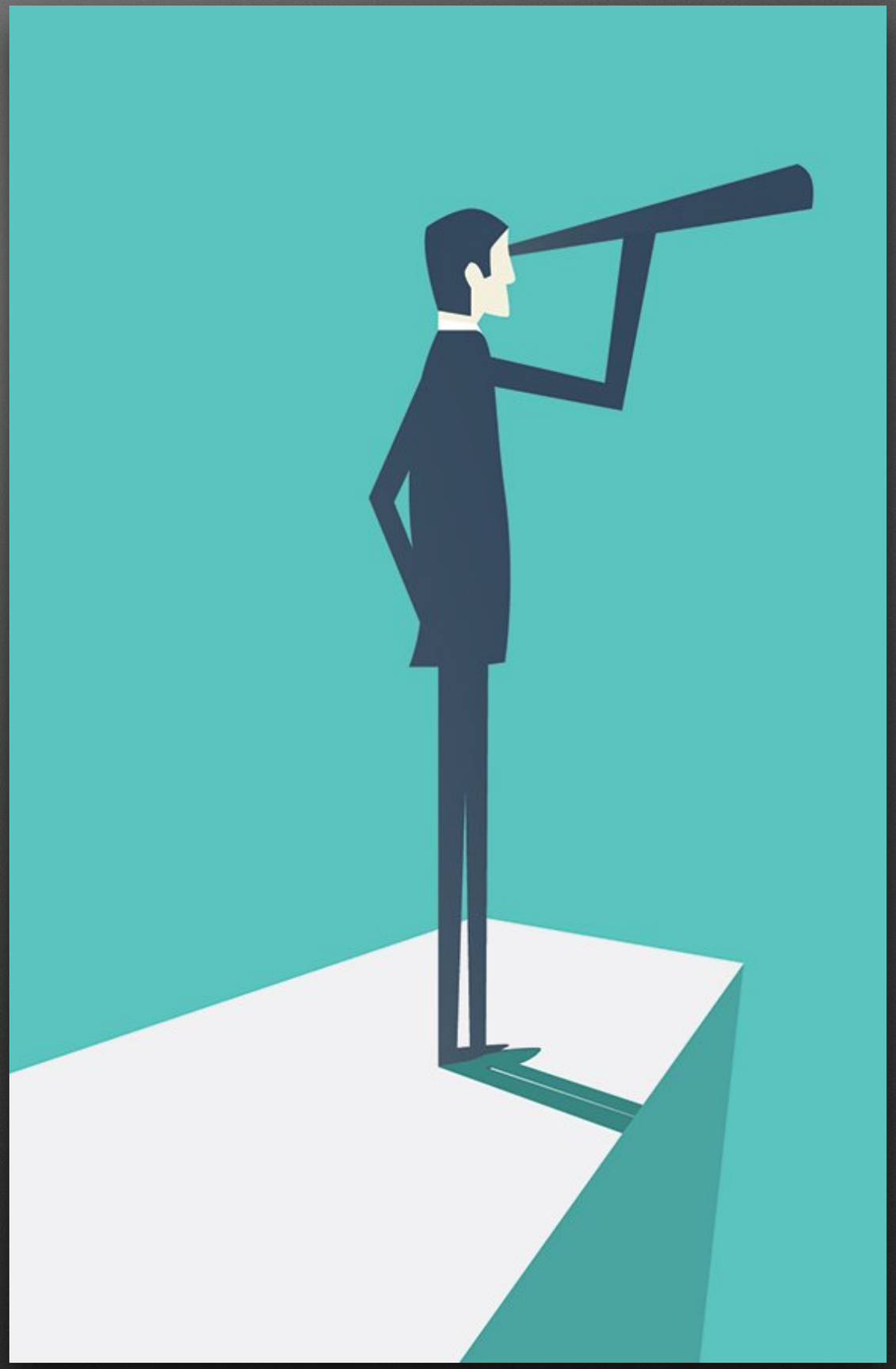


Overview

The Bombshell

The Bad News

It Gets Worse



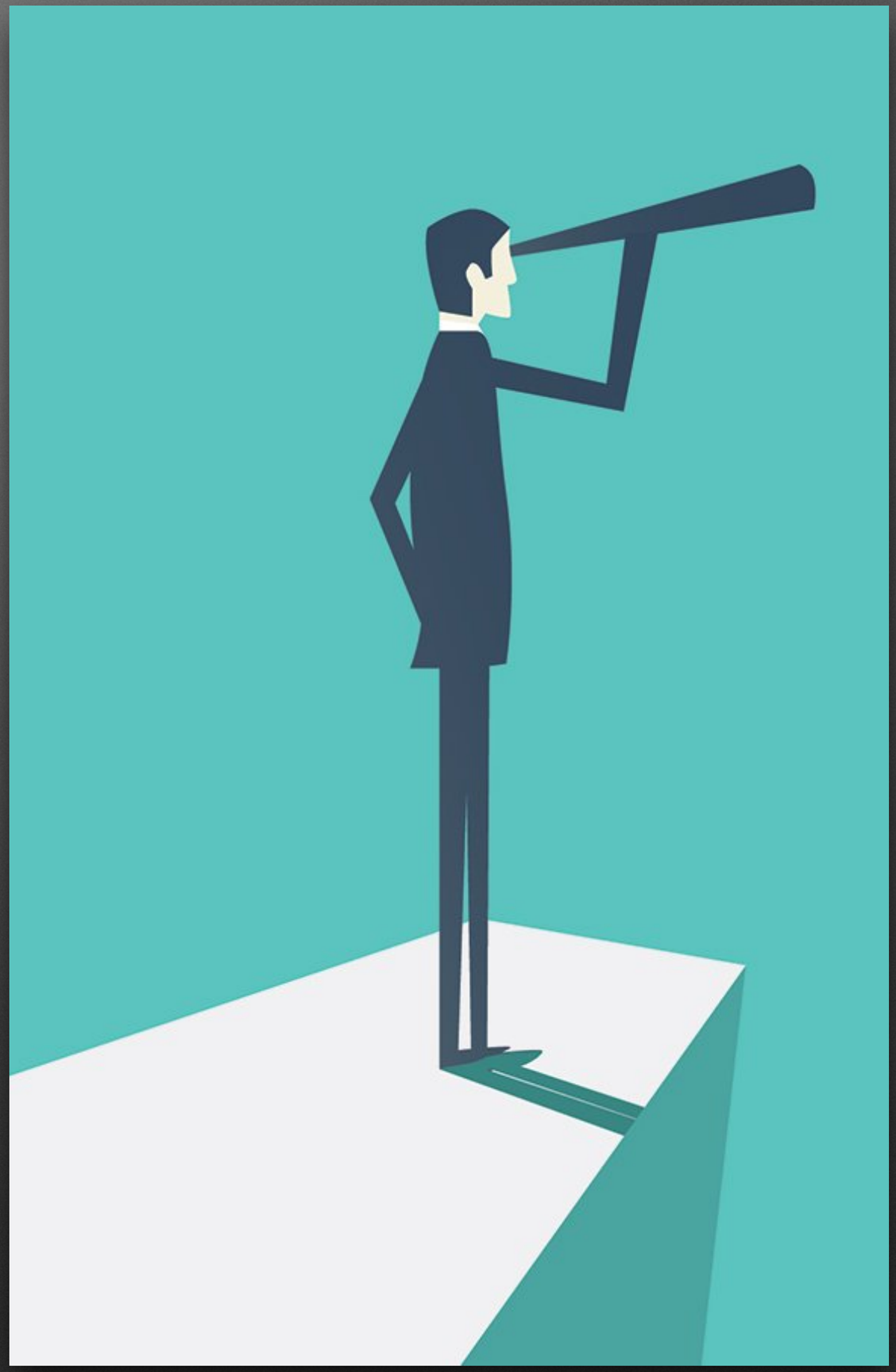
Overview

The Bombshell

The Bad News

It Gets Worse

Some Good News



Overview

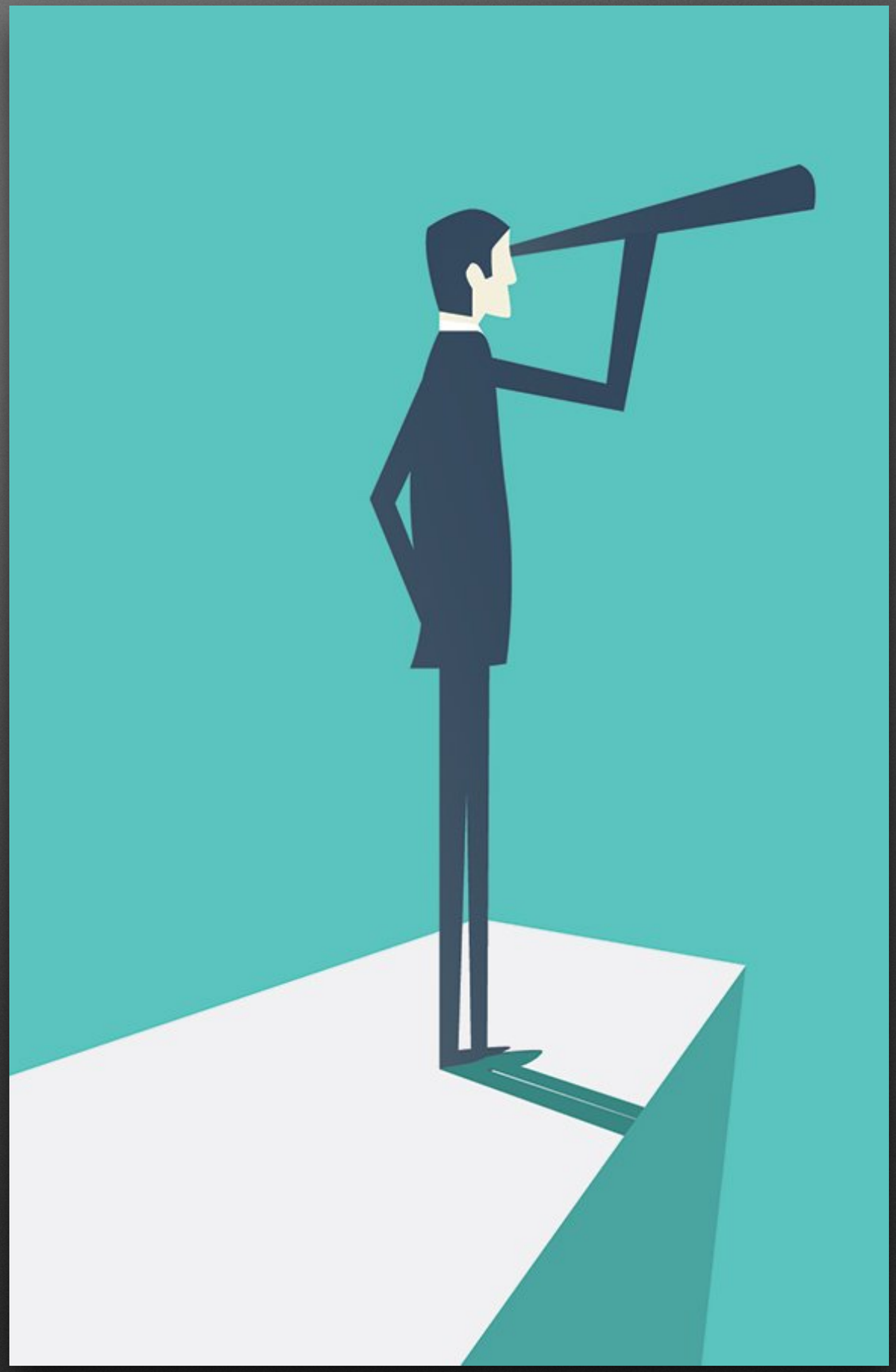
The Bombshell

The Bad News

It Gets Worse

Some Good News

What You Can Do



Overview

The Bombshell

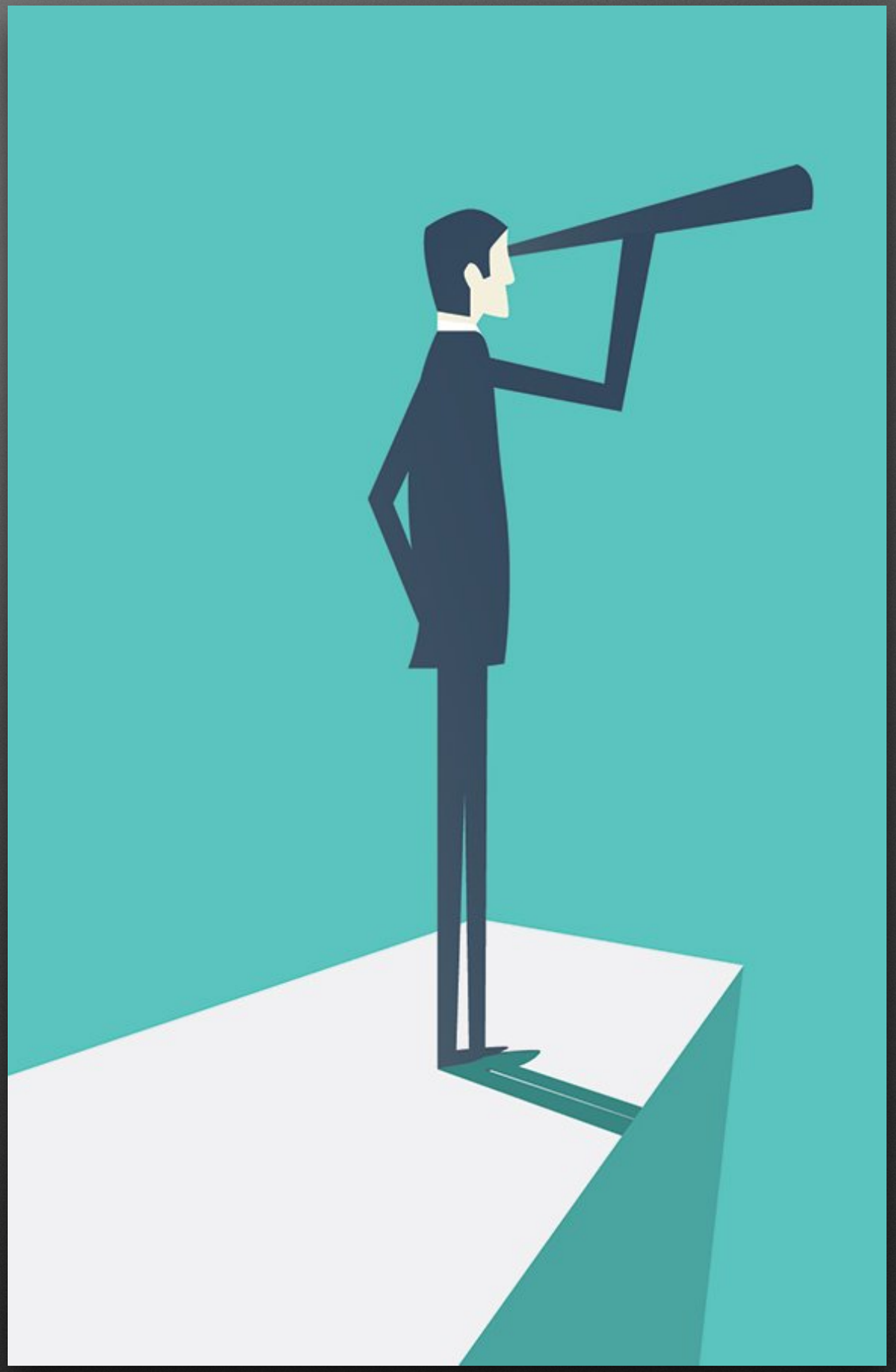
The Bad News

It Gets Worse

Some Good News

What You Can Do

Questions



The Bombshell

BUCKEYE —

Stolen NSA hacking tools were used in the wild 14 months before Shadow Brokers leak

Already criticized for not protecting its exploit arsenal, the NSA has a new lapse.

DAN GOODIN - 5/7/2019, 1:14 AM

707,510 views | Jul 20, 2019, 12:39pm

Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach In Its History'

Zak Doffman Contributor

Cybersecurity

I write about security and surveillance.

https://www.forbes.com/sites/zakdoffman/2019/07/20/russian-intelligence-has-been-hacked-with-social-media-and-tor-projects-exposed/

The Bad News

SECURITY

Stolen NSA hacking tool now victimizing US cities, report says

The EternalBlue hacking exploit, already used in the infamous WannaCry and NotPetya attacks, has now surfaced in the NSA's own backyard, says The New York Times.

BY EDWARD MOYER | MAY 25, 2019 12:45 PM PDT

0

Finding our personal data on the dark web 00:00/03:53

The Bad News

The City of Baltimore

The Bad News

The City of Baltimore

Hit by a major cyberattack

The Bad News

The City of Baltimore

Hit by a major cyberattack

Tool used was “EternalBlue”

The Bad News

The City of Baltimore

Hit by a major cyberattack

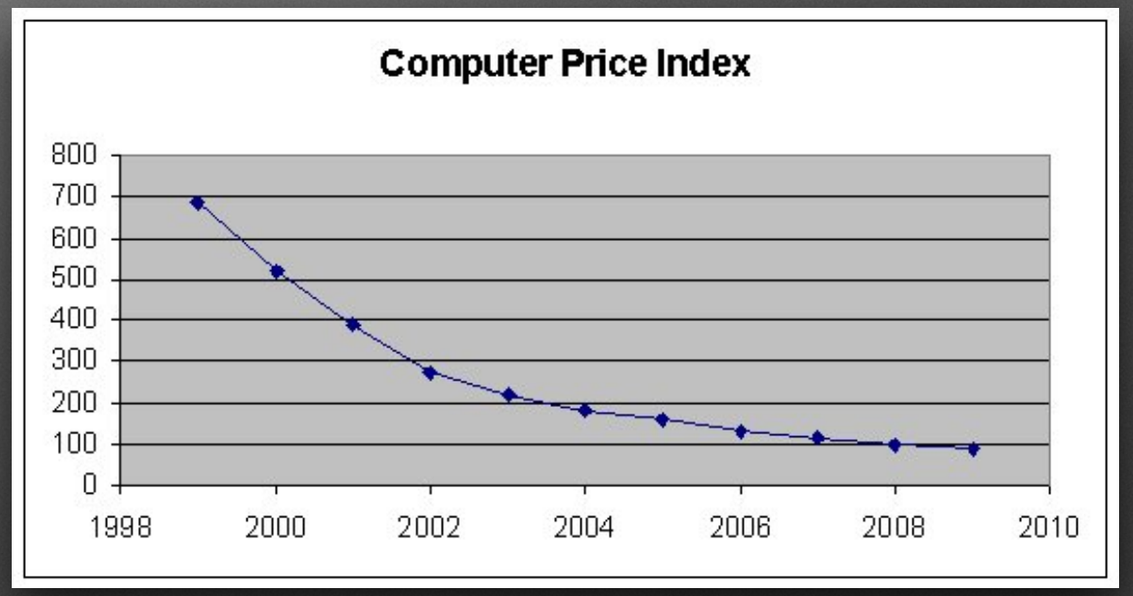
Tool used was “EternalBlue”

EternalBlue was developed by the NSA

It Gets Worse

It Gets Worse

The City of Baltimore
Hit by a major cyberattack
Tool used was “EternalBlue”
EternalBlue was developed by the NSA
Cost of EternalBlue will *drop*

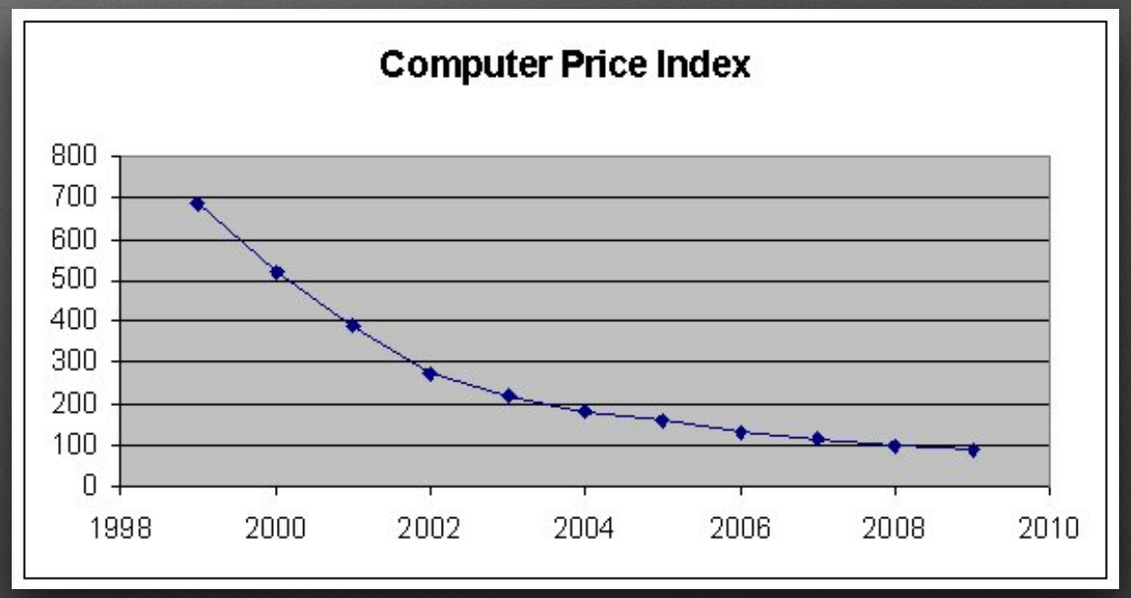


LOWEST COST OF ENTRY

EASY RAMP UP/SCALE DOWN

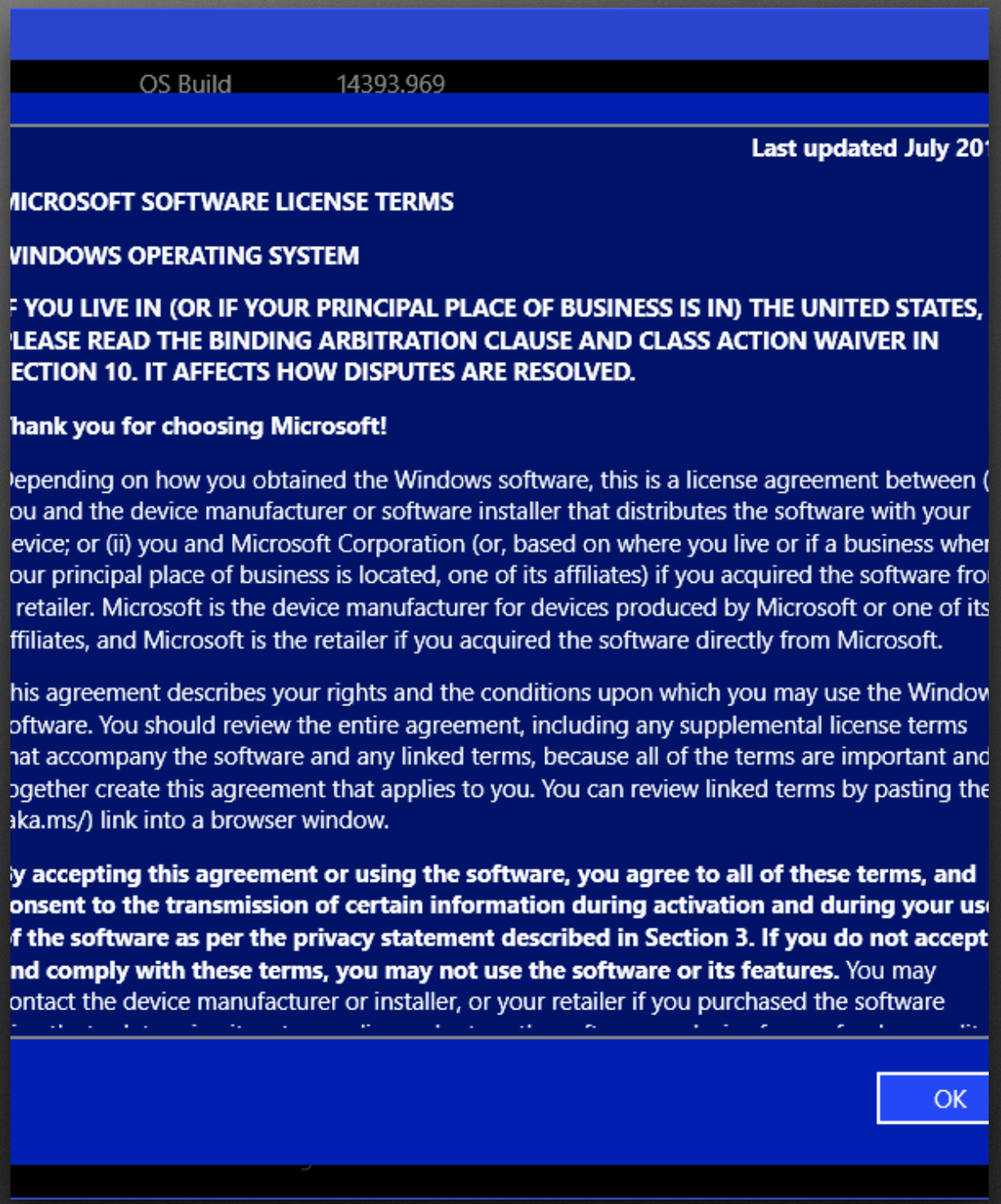
It Gets Worse

The City of Baltimore
Hit by a major cyberattack
Tool used was “EternalBlue”
EternalBlue was developed by the NSA
Cost of EternalBlue will *drop*
Law firms will be targeted by same tools



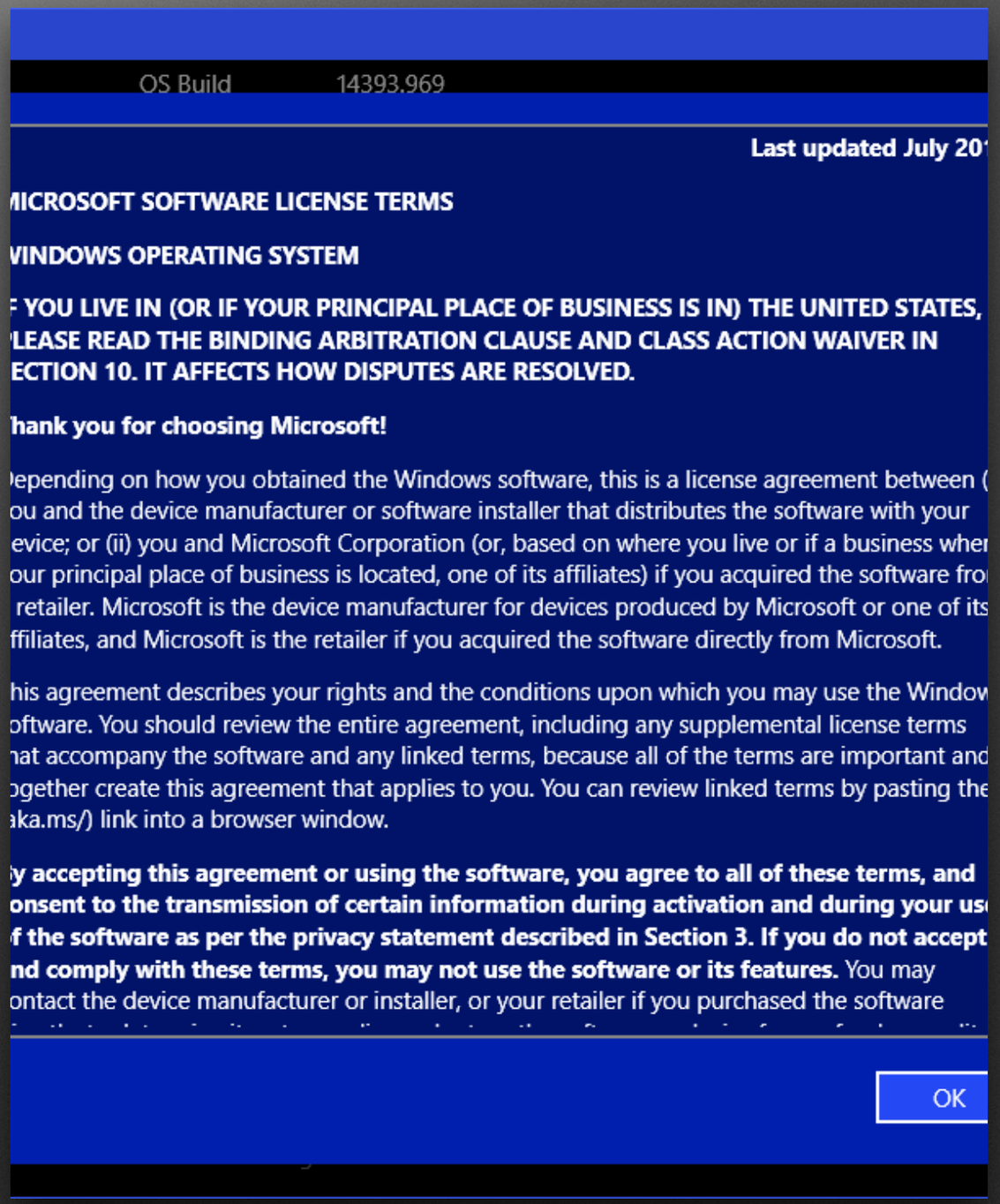
Even Worse

Software is monitized by data gathering (aka spying)



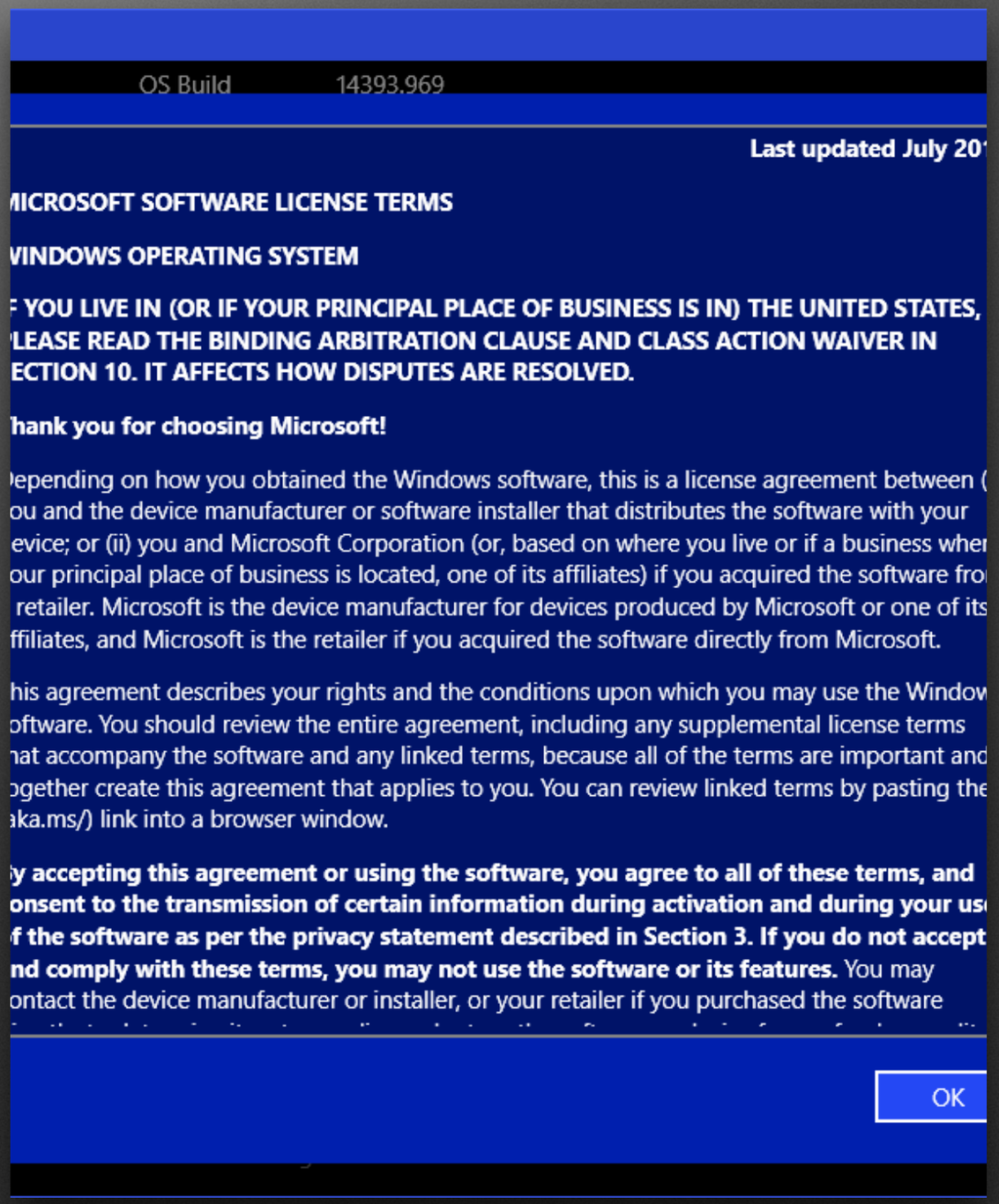
Software is monitized by data gathering (aka spying)

- To keep prices low (or free), a provider issues the software with the proviso that you allow them to spy on you and sell the resulting data



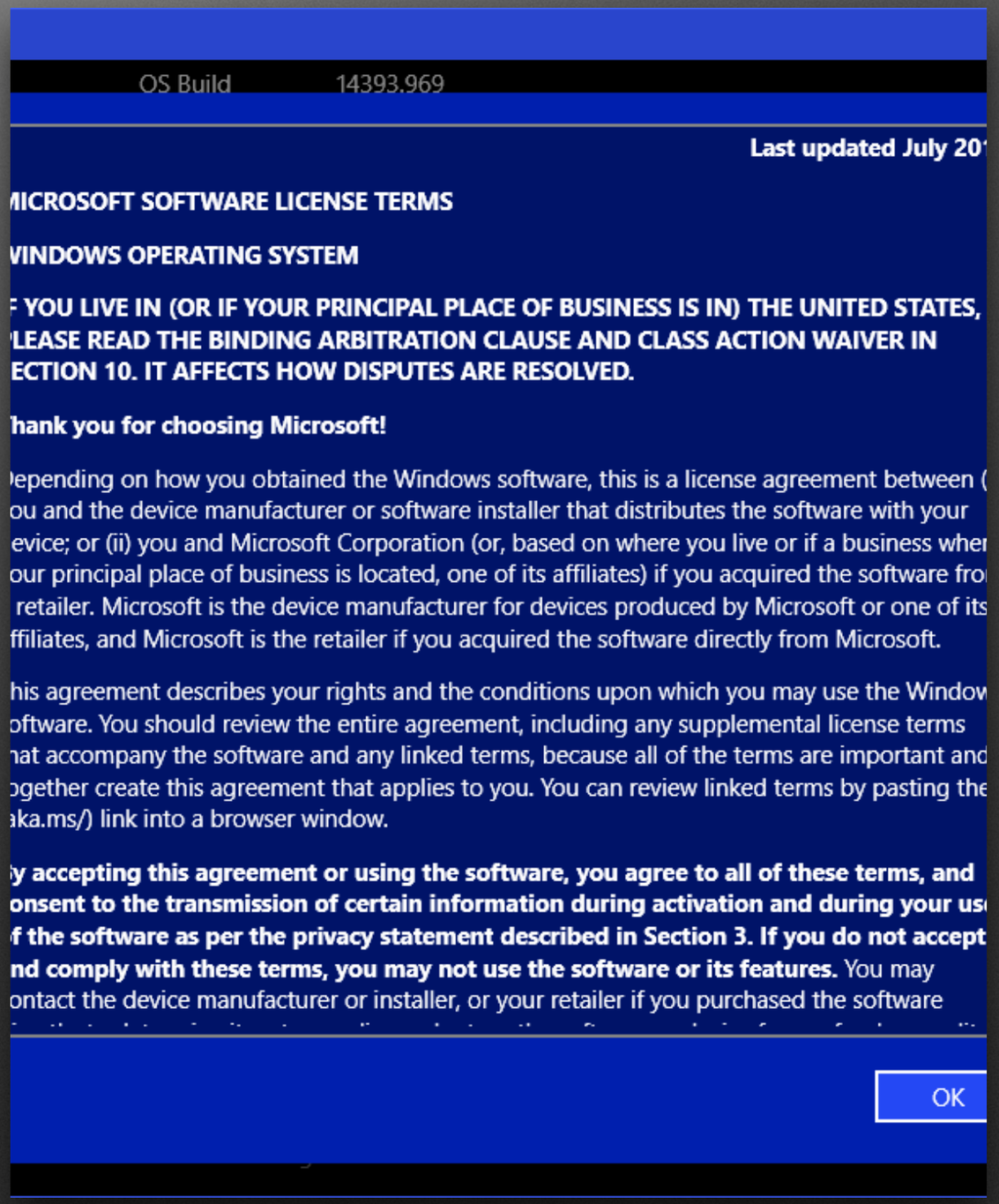
Software is monitized by data gathering (aka spying)

- To keep prices low (or free), a provider issues the software with the proviso that you allow them to spy on you and sell the resulting data
- The details are often buried in an End User License Agreement (EULA) that nobody reads



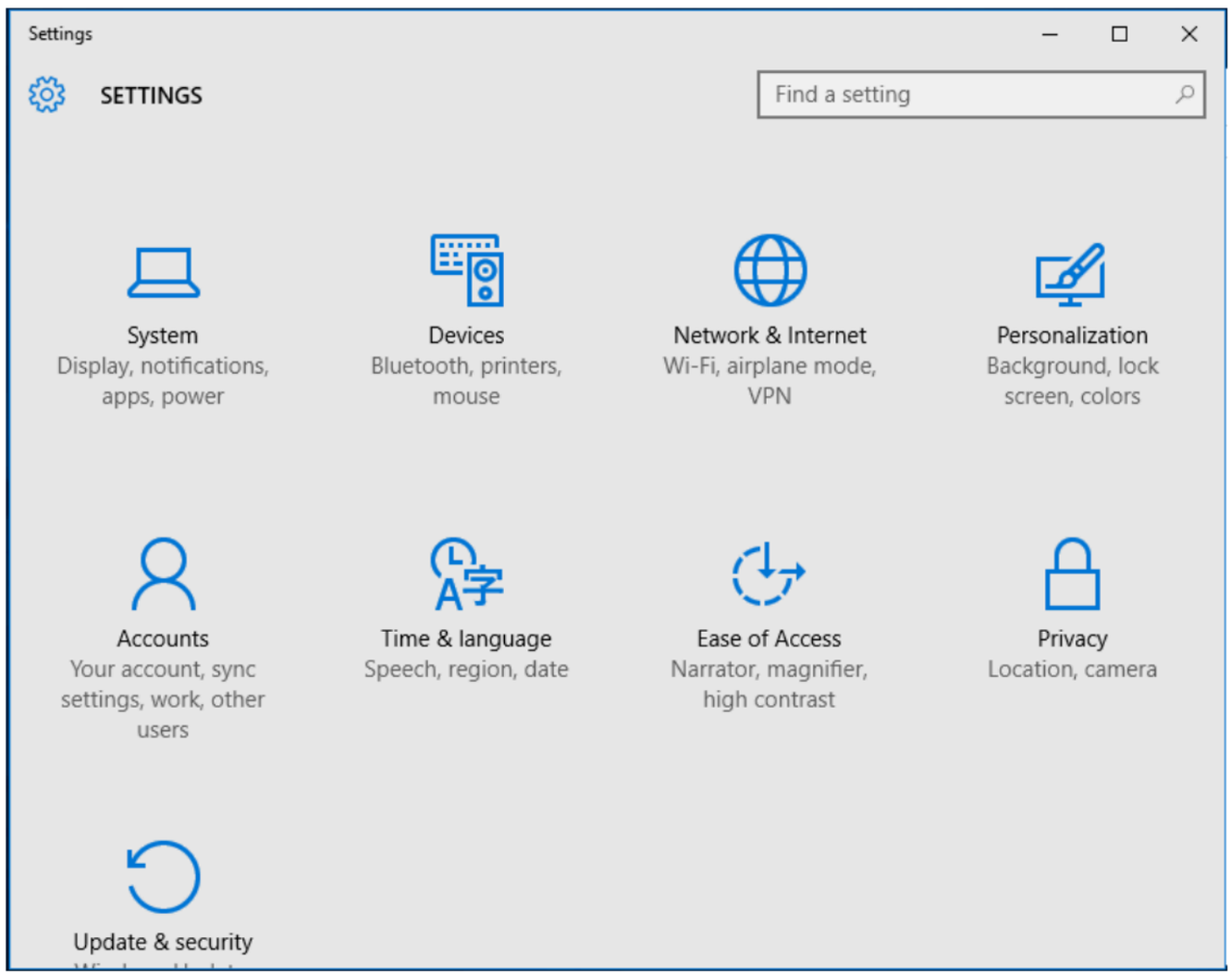
Software is monitized by data gathering (aka spying)

- To keep prices low (or free), a provider issues the software with the proviso that you allow them to spy on you and sell the resulting data
- The details are often buried in an End User License Agreement (EULA) that nobody reads
- Many online services do this, but now even operating systems have resorted to this



Windows 10 and HIPAA Security Officer Compliance

september 22, 2015 by steven marco • 6 comments

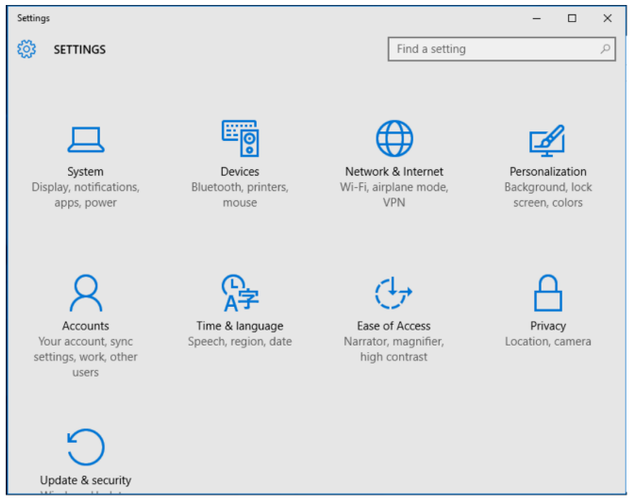


CIOs, IT Directors and IT Managers are often deputized as their organization's HIPAA Security Officer. In

https://hipaaone.com/windows-10-and-hipaa/

Windows 10 and HIPAA Security Officer Compliance

september 22, 2015 by steven marco · 6 comments



CIOs, IT Directors and IT Managers are often deputized as their organization's HIPAA Security Officer. In

https://hipaaone.com/windows-10-and-hipaa/

The short answer is that the default configuration of Windows 10 *may* violate HIPAA. The Windows 10 Privacy Statement as part of the Microsoft License terms July 2015 provides very flexible language on how Personal Data is collected, used and shared. Specifically this provision states:

"We will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to protect our customers or enforce the terms governing the use of the services."


amazon


amazon


amazon

Hi, I'm Cortana.

United States Patent Application ***20190156818***

Kind Code **A1**

Piersol; Kurt Wesley ; et al. **May 23, 2019**

PRE-WAKEWORD SPEECH PROCESSING

Abstract

A system for capturing and processing portions of a spoken utterance command that may occur before a wakeword. The system buffers incoming audio and indicates locations in the audio where the utterance changes, for example when a long pause is detected. When the system detects a wakeword within a particular utterance, the system determines the most recent utterance change location prior to the wakeword and sends the audio from that location to the end of the command utterance to a server for further speech processing.

Inventors: **Piersol; Kurt Wesley**; *(San Jose, CA)* **; Beddingfield; Gabriel**; *(Fremont, CA)*

Applicant:

Name	City	State	Country	Type
Amazon Technologies, Inc.	Seattle	WA	US	

Family ID: **65032116**

Appl. No.: **16/256376**

Filed: **January 24, 2019**

Related U.S. Patent Documents

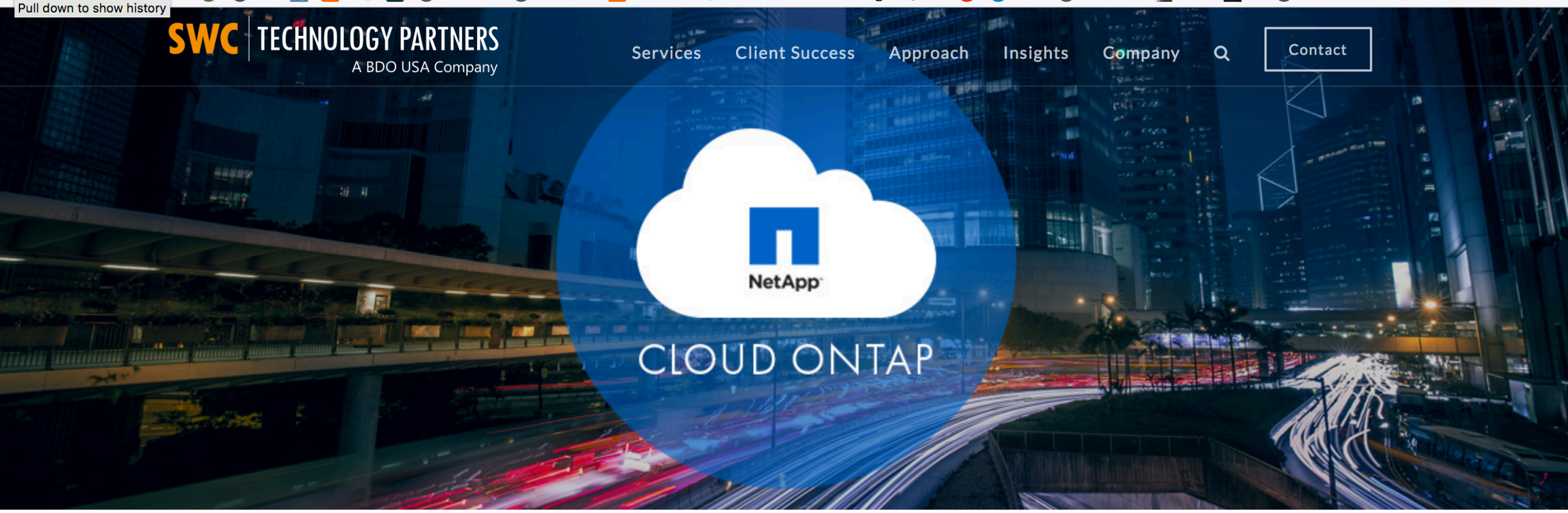
Application Number	Filing Date	Patent Number
14672277	Mar 30, 2015	10192546


Google
Play Store
Google Photos
Google Keep
Google Maps
Chrome
Calendar
Files
All apps
12:45
SAMSUNG

Is it safe to store corporate information on Google Drive (or similar services)?

When it comes to protecting corporate information, some doubt whether or not the cloud is the best option. We look at all the security services available.

Josep Albors 26 Jul 2017 - 02:00PM



WRITTEN BY
Jeff Lanham

CUSTOMER DATA CONFIDENTIALITY IN MICROSOFT OFFICE 365

JULY 21, 2015 // CLOUD
AZURE, CLOUD, DATA, OFFICE 365, SECURITY

As more organizations consider moving some (or all) of their information technology out of

Some Good News

Announcing Customer Lockbox for Office 365

By the Office 365 team, on April 21, 2015

Editor's note 10/7/2015
The FAQs have been updated to provide more clarification.

Editor's note 8/5/2015
The FAQs have been updated with Customer Lockbox purchase information.

This post was written by Vijay Kumar, senior product marketing manager, and Raji Dani, principal program manager for the Office 365 Security team.

As a cloud services provider, we recognize that organizations understandably want to have full control over access to their content stored in cloud services. Today at RSA, we announced Customer Lockbox for Office 365, a new capability designed to provide customers with unprecedented control over their content in the service. Customer Lockbox gives customers explicit control in the very rare instances when a Microsoft engineer may need access to customer content to resolve a customer issue.

In our efforts to maximize data security and privacy for Office 365 customers, we have engineered the service to require nearly zero interaction with customer content by Microsoft employees. Nearly all service operations performed by Microsoft are fully automated and the human involvement is highly controlled and abstracted away from customer content. As a result, only in rare cases—such as when troubleshooting a customer issue with mailbox or document contents—does a Microsoft engineer have any reason to access customer content in Office 365.


IMPORTANT

The Key is *Privity*

No client data when you *assented* to the EULA

Did your client assent to (later) third-party access to their data?

The third-party is relying on your *apparent* authority when they access the client's data

No *privity* between the third-party and your client

If there is a problem, the *attorney* gets in trouble

Legal Analogies

Legal Analogies

- Texas Disciplinary Rule 1.05

Legal Analogies

- Texas Disciplinary Rule 1.05
- Data Breach/Notification Statutes (Tex. Bus. & Comm. Code)

Legal Analogies

- Texas Disciplinary Rule 1.05
- Data Breach/Notification Statutes (Tex. Bus. & Comm. Code)
- Trade Secrets (Tex. UTSA in the Civ. Prac. & Rem. Code)

Legal Analogies

- Texas Disciplinary Rule 1.05
- Data Breach/Notification Statutes (Tex. Bus. & Comm. Code)
- Trade Secrets (Tex. UTSA in the Civ. Prac. & Rem. Code)
- Third Party Doctrine of the Fourth Amendment

Legal Analogies

- Texas Disciplinary Rule 1.05
- Data Breach/Notification Statutes (Tex. Bus. & Comm. Code)
- Trade Secrets (Tex. UTSA in the Civ. Prac. & Rem. Code)
- Third Party Doctrine of the Fourth Amendment
- HIPAA / HITEC Act / GLBA

Things To Do

Things To Do

Adopt a heterogenous computing environment

Things To Do

Adopt a heterogenous computing environment

Prepare backup systems for major cyberattacks

Things To Do

Adopt a heterogenous computing environment

Prepare backup systems for major cyberattacks

CYA - Include a clause in your engagement agreement about third-party software & data services

Things To Do

Adopt a heterogenous computing environment

Prepare backup systems for major cyberattacks

CYA - Include a clause in your engagement agreement about third-party software & data services

Utilize what third-party applications allow to enhance confidentiality of the client's information

Questions?

Questions?

Ronald L. Chichester

Ron@TexasComputerLaw.com

713-302-1679

Principles of Cyber Law and Policy

Created by **Kevin Kuczynski** - **Penn State University** , updated 4/9/19

Contributors: **James Houck** - **Penn State**, **Anne Mckenna** - **Penn State University, Dickinson Law**, **Scott Sigmund Gartner** - **Penn State School Of International Affairs**

Course

NSA NCCP

NOT AVAILABLE FOR DOWNLOAD

SAVE TO LIBRARY

Please log in to add this Learning Object to your library.

13 saves 5 downloads

Attribute this Object

"Principles of Cyber Law and Policy" by Kevin Kuczynski is

Description

Principles of Cyber Operations Law and Policy Course.

Consists of the following modules:

- Module I Understanding Cyberspace
- Module II Cyber Governance: Three Branches of Government
- Module III Legal Foundations of Modern Cyber Law and Policy
- Module IV Cyber Operations

https://clark.center/details/kkuczynski/Principles%20of%20Cyber%20Law%20and%20Policy

(It's Free)